aws

Manual do usuário

Amazon Virtual Private Cloud

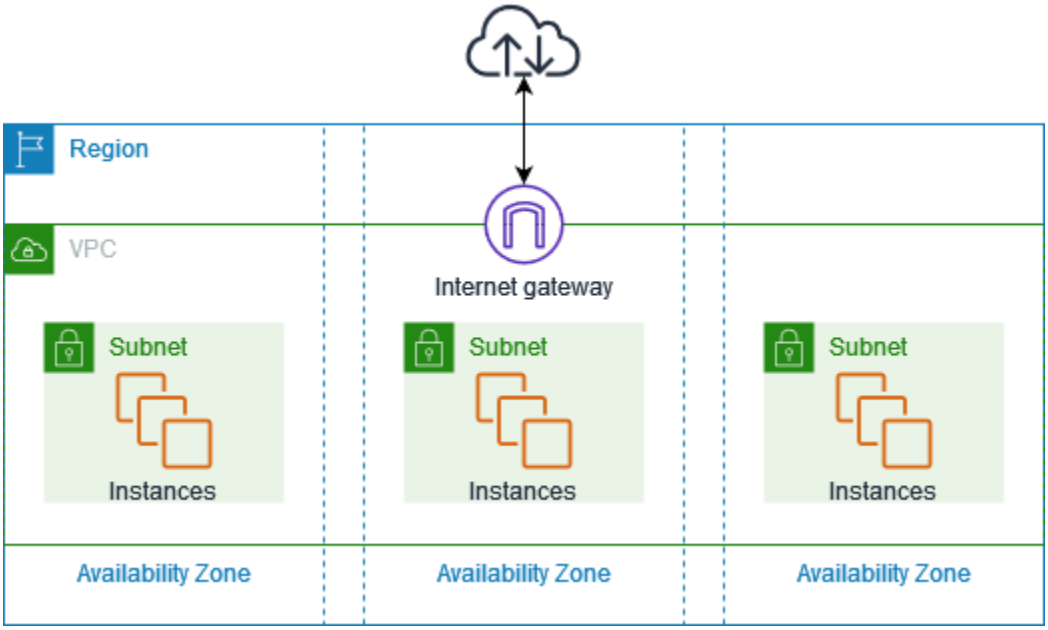
Amazon Virtual Private Cloud: Manual do usuário

Table of Contents

O que é Amazon VPC?

Com a Amazon Virtual Private Cloud (Amazon VPC), é possível iniciar recursos da AWS em uma rede virtual logicamente isolada que você mesmo define. Essa rede virtual se assemelha a uma rede tradicional que você operaria no seu data center, com os benefícios de usar a infraestrutura escalável da AWS.

O seguinte diagrama mostra uma VPC de exemplo. A VPC tem: uma sub-rede em cada zona de disponibilidade na região, instâncias do EC2 em cada sub-rede e um gateway da Internet para facilitar a comunicação entre os recursos em sua VPC e a Internet.



Para obter mais informações, consulte Amazon Virtual Private Cloud (Amazon VPC).

Recursos

Os recursos a seguir ajudam você a configurar uma VPC para fornecer a conectividade de que as aplicações precisam:

Nuvens privadas virtuais (VPC)

A VPC é uma rede virtual muito semelhante a uma rede tradicional que você pode operar no seu próprio data center. Após criar uma VPC, você pode adicionar sub-redes.

Sub-redes

Uma sub-rede consiste em um intervalo de endereços IP na VPC. Cada sub-rede fica alocada em uma única zona de disponibilidade. Após adicionar as sub-redes, você pode implantar os recursos da AWS na VPC.

Endereçamento IP

É possível atribuir endereços IP, tanto IPv4 quanto IPv6, às VPCs e sub-redes. Você também pode trazer os endereços GUA IPv6 e IPv4 públicos para a AWS e alocá-los nos recursos da VPC, como instâncias do EC2, gateways NAT e balanceadores de carga da rede.

Roteamento

Use tabelas de rotas para direcionar o tráfego da sub-rede ou do gateway.

Gateways e endpoints

Um gateway conecta a VPC a uma outra rede. Por exemplo, use um gateway da Internet para conectar a VPC à Internet. Use um endpoint da VPC para se conectar a Serviços da AWS de modo privado, sem usar um gateway da Internet ou um dispositivo NAT.

Conexões de emparelhamento

Use uma conexão de emparelhamento da VPC para rotear o tráfego entre os recursos em duas VPCs.

Espelhamento de tráfego

Copie o tráfego de rede das interfaces de rede e envie aos dispositivos de segurança e monitoramento para inspeção profunda dos pacotes.

Gateways de trânsito

Use um gateway de trânsito, que funciona como um hub central, para rotear tráfego entre VPCs, conexões VPN e conexões do AWS Direct Connect.

Logs de fluxo da VPC

Um log de fluxo capta informações sobre o tráfego IP que entra e sai das interfaces de rede da VPC.

Conexões da VPN

Conecte as VPCs às suas redes on-premises usando a AWS Virtual Private Network (AWS VPN) .

Conceitos básicos da Amazon VPC

Toda Conta da AWS inclui uma VPC padrão em cada Região da AWS. As VPCs padrão são configuradas de modo que você possa começar imediatamente a iniciar instâncias do EC2 e conectar-se a elas. Para ter mais informações, consulte Como planejar a VPC.

Você pode optar por criar VPCs adicionais com as sub-redes, os endereços IP, os gateways e o roteamento necessários. Para ter mais informações, consulte the section called “Crie uma VPC”.

Trabalhar com a Amazon VPC

Você pode criar e gerenciar as VPCs usando qualquer uma das seguintes interfaces:

- AWS Management Console: fornece uma interface web para acessar as VPCs.
- AWS Command Line Interface (AWS CLI): fornece comandos para um amplo conjunto de serviços da AWS, inclusiva a Amazon VPC, e é compatível com Windows, Mac e Linux. Para obter mais informações, consulte AWS Command Line Interface.
- AWS SDKs: fornecem APIs para linguagens de programação específicas e cuidam de muitos dos detalhes da conexão, como cálculo de assinaturas, tratamento de novas tentativas de solicitação e tratamento de erros. Para obter mais informações, consulte AWS SDKs.
- API de consulta: fornece ações de API técnicas que você aciona usando solicitações HTTPS. Usar a API de consulta é a maneira mais direta para acessar a Amazon VPC, mas exige que a própria aplicação lide com detalhes técnicos, como gerar o hash para assinar a solicitação e tratamento de erros. Para mais informações, consulte Ações da Amazon VPC na Referência de API do Amazon EC2.

Precificação da Amazon VPC

Não há custo adicional por usar a VPC. Porém, alguns componentes da VPC são cobrados, como os gateways NAT, o Gerenciador de Endereços IP, o espelhamento de tráfego, o Analisador de Acessibilidade e o Analisador de Acesso à Rede. Para obter mais informações, consulte Precificação da Amazon VPC.

Quase todos os recursos que você inicia na nuvem privada virtual (VPC) portam um endereço IP para fins de conectividade. A maioria dos recursos na VPC usa endereços IPv4 privados, porém os recursos que exigem acesso direto à Internet por IPv4 usam endereços IPv4 públicos.

A Amazon VPC permite a você inicializar serviços gerenciados, como o Elastic Load Balancing, o Amazon RDS e o Amazon EMR, sem ter uma VPC configurada previamente. Isso é feito usando a VPC padrão em sua conta, se você tiver uma. Todos os endereços IPv4 públicos provisionados à sua conta pelo serviço gerenciado serão cobrados. Essas cobranças serão associadas ao serviço da Amazon VPC em seu AWS Cost and Usage Report.

Precificação de endereços IPv4 públicos

Um endereço IPv4 público é um endereço IPv4 que pode ser roteado a partir da Internet. É necessário um endereço IPv4 público para um recurso poder ser acessado diretamente da Internet via IPv4.

Todo cliente do nível gratuito da AWS recebe 750 horas de uso de endereços IPv4 públicos sem custos com o serviço do EC2. Caso você não use o serviço do EC2 no nível gratuito da AWS, os endereços IPv4 públicos serão cobrados. Para obter informações específicas sobre preços, consulte a guia Endereço IPv4 público em Precificação da Amazon VPC.

Endereços IPv4 privados (RFC 1918) não são cobrados. Para mais informações sobre como endereços IPv4 públicos são cobrados em VPCs compartilhadas, consulte Cobrança e medição para o proprietário e os participantes.

Estes são os tipos de endereços IPv4 públicos:

- Endereços IP elásticos (EIPs): endereços IPv4 públicos estáticos fornecidos pela Amazon que você pode associar a uma instância do EC2, interface de rede elástica ou recurso da AWS.
- Endereços IPv4 públicos do EC2: endereços IPv4 públicos atribuídos a uma instância do EC2 pela Amazon (se a instância do EC2 for iniciada em uma sub-rede padrão ou for executada em uma sub-rede configurada para atribuir automaticamente um endereço IPv4 público).
- Endereços BYOIPv4: endereços IPv4 públicos no intervalo de endereços IPv4 que você trouxe para a AWS usando o recurso Traga seus próprios endereços IP (BYOIP).
- Endereços IPv4 gerenciados por serviços: endereços IPv4 públicos provisionados automaticamente em recursos da AWS e gerenciados por um serviço da AWS. Por exemplo, endereços IPv4 públicos no Amazon ECS, no Amazon RDS ou no Amazon WorkSpaces.

A seguinte lista mostra os serviços da AWS mais comuns que podem usar endereços IPv4 públicos.

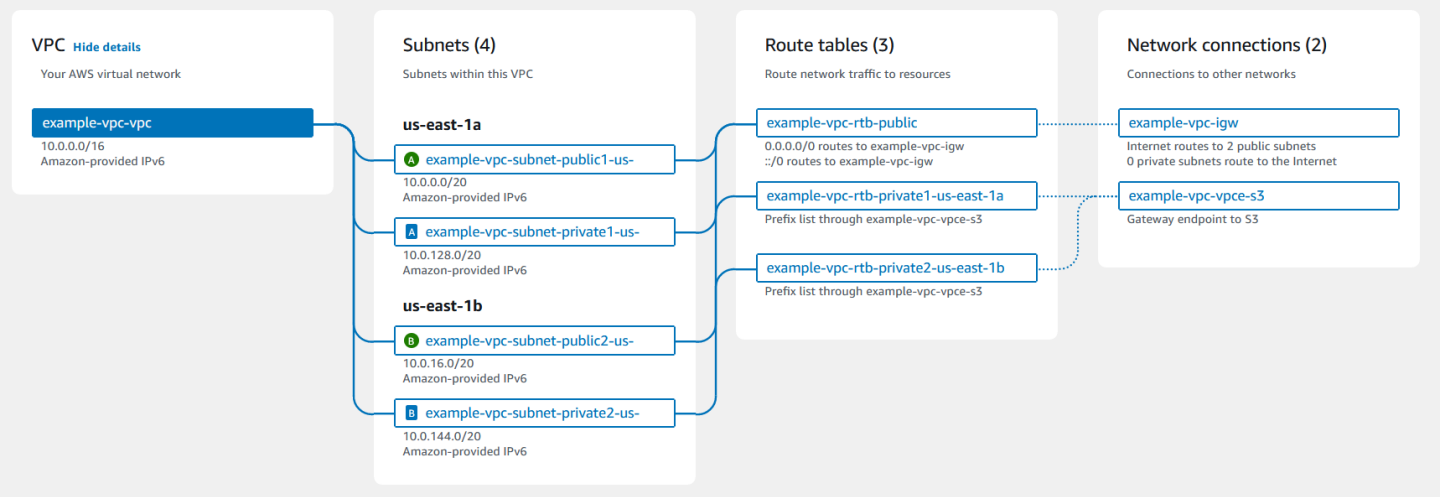
- Amazon AppStream 2.0
- AWS Client VPN

- AWS Database Migration Service
- Amazon EC2
- Amazon Elastic Container Service
- Amazon EKS
- Amazon EMR
- Amazon GameLift
- AWS Global Accelerator
- AWS Mainframe Modernization
- Amazon Managed Streaming for Apache Kafka
- Amazon MQ
- Amazon RDS
- Amazon Redshift
- AWS Site-to-Site VPN
- Gateway NAT da Amazon VPC
- Amazon WorkSpaces
- Elastic Load Balancing

Como funciona a Amazon VPC

Com a Amazon Virtual Private Cloud (Amazon VPC), é possível iniciar recursos da AWS em uma rede virtual logicamente isolada que você mesmo define. Essa rede virtual se assemelha a uma rede tradicional que você operaria no seu data center, com os benefícios de usar a infraestrutura escalável da AWS.

A seguir há uma representação visual de uma VPC e seus recursos no painel Visualização mostrado quando você cria uma VPC usando o AWS Management Console. Para uma VPC existente, é possível acessar essa visualização na guia Mapa de recursos. Este exemplo mostra os recursos inicialmente selecionados na página Criar VPC quando você escolhe criar a VPC e outros recursos de rede. Essa VPC é configurada com um CIDR IPv4 e um CIDR IPv6 fornecido pela Amazon, sub-redes em duas zonas de disponibilidade, três tabelas de rotas, um gateway da Internet e um endpoint de gateway. Como selecionamos o gateway da Internet, a visualização indica que o tráfego das sub-redes públicas é roteado para a Internet porque a tabela de rotas correspondente envia o tráfego para o gateway da Internet.



Conceitos

- VPCs e sub-redes
- VPCs padrão e não padrão
- Tabelas de rotas
- Acesso à Internet
- Acessar uma rede corporativa ou doméstica
- Conectar VPCs e redes

- Rede global privada da AWS

VPCs e sub-redes

Uma nuvem privada virtual (VPC) é uma rede virtual dedicada à sua conta da AWS. Ela é isolada de maneira lógica de outras redes virtuais na Nuvem da AWS. Você pode especificar um intervalo de endereços IP para a VPC, adicionar sub-redes, adicionar gateways e associar grupos de segurança.

Uma sub-rede consiste em um intervalo de endereços IP na VPC. Você inicia recursos da AWS, como instâncias do Amazon EC2, nas suas sub-redes. É possível conectar uma sub-rede à Internet, outras VPCs e aos seus próprios data centers e rotear tráfego de e para as suas sub-redes utilizando tabelas de rotas.

Saiba mais

- Endereçamento IP
- Nuvens privadas virtuais
- Sub-redes

VPCs padrão e não padrão

Se a sua conta foi criada após 4 de dezembro de 2013, ela vem com uma VPC padrão em cada região. Uma VPC padrão está configurada e pronta para uso. Por exemplo, ela tem uma sub-rede padrão em cada zona de disponibilidade da região, um gateway da Internet anexado, uma rota na tabela de rotas principal que envia todo o tráfego para o gateway da Internet e configurações de DNS que atribuem automaticamente nomes de hosts DNS públicos a instâncias com endereços IP públicos e habilitam a resolução de DNS por meio do servidor de DNS fornecido pela Amazon (consulte Atributos de DNS para sua VPC). Portanto, uma instância do EC2 iniciada em uma sub-rede padrão automaticamente tem acesso à Internet. Se você tiver uma VPC padrão em uma região e não especificar uma sub-rede quando iniciar uma instância do EC2 naquela região, uma das sub-redes padrão será escolhida e a instância será iniciada nessa sub-rede.

Você também pode criar sua própria VPC e configurá-la conforme necessário. Isso é conhecido como uma VPC não padrão. As sub-redes criadas na VPC não padrão e as sub-redes adicionais criadas na VPC padrão são chamadas de sub-redes não padrão.

Saiba mais

- the section called “VPCs padrão”
- the section called “Crie uma VPC”

Tabelas de rotas

Uma tabela de rotas contém um conjunto de regras chamado de rotas, as quais são usadas para determinar para onde o tráfego de rede da VPC é direcionado. Você pode associar explicitamente uma sub-rede a uma tabela de rotas específica. Caso contrário, a sub-rede é implicitamente associada à tabela de rotas principal.

Cada rota em uma tabela de rotas especifica o intervalo de endereços IP para onde você deseja que o tráfego vá (o destino) e o gateway, a interface de rede ou a conexão por meio da qual enviar o tráfego (o destino).

Saiba mais

- Configurar tabelas de rotas

Acesso à Internet

Controle o modo como as instâncias executadas em uma VPC acessam os recursos fora da VPC.

Uma VPC padrão inclui um gateway da Internet e cada sub-rede padrão é uma sub-rede pública. Cada instância executada em uma sub-rede padrão possui dois endereços IPv4: um público e outro privado. Essas instâncias podem se comunicar com a Internet através do gateway da Internet. Um gateway da Internet permite que as instâncias se conectem à Internet por meio da borda de rede do Amazon EC2.

Em regra, cada instância executada em uma sub-rede não padrão tem apenas um endereço IPv4 privado. Para haver o endereço público IPv4 será preciso atribuir especificamente um no momento da execução ou modificar o atributo do endereço IP público da sub-rede. Essas instâncias podem se comunicar entre si, mas não podem acessar a Internet.

Habilite o acesso à Internet para uma instância executada em uma sub-rede não padrão anexando um gateway da Internet à sua VPC (caso essa não seja padrão) e associando um endereço IP elástico à instância.

Como alternativa, para permitir que uma instância na VPC inicie as conexões de saída para a Internet, mas também evitar as conexões de entrada não solicitadas pela Internet, use um dispositivo de Network Address Translation (NAT – Tradução de endereços de rede). O NAT mapeia vários endereços IPv4 privados para um único endereço público IPv4. Você pode configurar um dispositivo de NAT com um endereço IP elástico e conectá-lo à Internet por meio de um gateway da Internet. Isso permite que uma instância em uma sub-rede privada se conecte à Internet via dispositivo de NAT, roteando tráfego da instância para um gateway da Internet e quaisquer respostas para a instância.

Se você associar um bloco CIDR IPv6 à sua VPC e atribuir endereços IPv6 às suas instâncias, as instâncias poderão se conectar à Internet via IPv6 por meio de um gateway de Internet. Alternativamente, as instâncias podem executar conexões de saída para a Internet via IPv6 usando um gateway da Internet somente de saída. Como há separação entre os tráfegos IPv4 e IPv6, as tabelas de rotas devem incluir rotas distintas para o tráfego IPv6.

Saiba mais

- Habilitar o acesso da VPC à Internet usando gateways da Internet
- Habilitar o tráfego IPv6 de saída usando gateways da Internet somente de saída
- Estabelecer conexão com a Internet ou a outras redes usando dispositivos NAT

Acessar uma rede corporativa ou doméstica

Como opção, você pode conectar sua VPC ao seu próprio data center corporativo usando uma conexão IPsec do AWS Site-to-Site VPN e transformando a Nuvem AWS em uma extensão do seu data center.

Uma conexão Site-to-Site VPN consiste em dois túneis de VPN entre um gateway privado virtual ou um gateway de trânsito no lado da AWS e um dispositivo de gateway do cliente localizado em seu data center. Um dispositivo de gateway do cliente é um dispositivo físico ou um software configurado no seu lado da conexão do Site-to-Site VPN.

Saiba mais

- Guia do usuário do AWS Site-to-Site VPN
- Gateways de trânsito da Amazon VPC

Conectar VPCs e redes

É possível criar uma conexão de emparelhamento de VPC entre duas VPCs que permite rotear o tráfego entre elas de forma privada. Instâncias em qualquer VPC podem se comunicar umas com as outras como se estivessem na mesma rede.

Você também pode criar um gateway de trânsito e usá-lo para interconectar as VPCs e redes on-premises. O gateway de trânsito atua como roteador virtual regional para o tráfego que flui entre seus anexos, o que pode incluir VPCs, conexões VPN, gateways do AWS Direct Connect e conexões de emparelhamento de gateway de trânsito.

Saiba mais

- Amazon VPC Peering Guide
- Gateways de trânsito da Amazon VPC

Rede global privada da AWS

A AWS fornece uma rede global privada de alta performance e baixa latência que proporciona um ambiente de computação em nuvem seguro para oferecer suporte às suas necessidades de redes. AWS As regiões são conectadas a diversos provedores de serviços de Internet (ISPs), bem como a uma estrutura da rede global privada, que fornece uma performance de rede melhor para o tráfego entre regiões enviado por clientes.

As seguintes considerações se aplicam:

- O tráfego que está em uma zona de disponibilidade, ou entre zonas de disponibilidade em todas as regiões, faz o roteamento pela rede global privada da AWS.
- O tráfego que está entre regiões sempre faz o roteamento pela rede global privada da AWS, exceto regiões da China.

Pode haver perda do pacote de rede devido a vários fatores, incluindo colisões de fluxo de rede, nível baixo de erros (Camada 2) e outras falhas de rede. Nós projetamos e operamos nossas redes de modo a minimizar a perda de pacotes. Medimos a taxa de perda de pacote (PLR) na estrutura global que conecta as regiões da AWS. Operamos nossa rede de backbone com meta de p99 da PLR por hora de menos do que 0,0001%.

Como planejar a VPC

Conclua as tarefas a seguir para se preparar para criar e conectar suas VPCs. Ao concluir, você estará pronto para implantar sua aplicação na AWS.

Tarefas

- Inscrever-se para uma Conta da AWS
- Verificar permissões
- Determine seus intervalos de endereços IP
- Selecione suas zonas de disponibilidade
- Planeje sua conectividade com a Internet
- Crie sua VPC
- Implantar a aplicação

Inscrever-se para uma Conta da AWS

Se você ainda não tem uma Conta da AWS, siga as etapas abaixo para criar uma.

Como cadastrar uma Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.

   Quando você se inscreve para uma Conta da AWS, um Usuário raiz da conta da AWS é criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AAWS envia um e-mail de confirmação depois que o processo de cadastramento é concluído. A qualquer momento, é possível exibir as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Verificar permissões

Para poder utilizar a Amazon VPC, é necessário que você tenha as permissões necessárias. Para ter mais informações, consulte Identity and Access Management para o Amazon VPC e Exemplos de políticas da Amazon VPC.

Determine seus intervalos de endereços IP

Os recursos na sua VPC se comunicam entre si e com recursos na Internet usando endereços IP. Ao criar VPCs e sub-redes, é possível selecionar seus intervalos de endereços IP. Quando você implanta recursos em uma sub-rede, como instâncias do EC2, eles recebem endereços IP do intervalo de endereços IP da sub-rede. Para ter mais informações, consulte Endereçamento IP.

Ao escolher um tamanho para sua VPC, considere quantos endereços IP você precisará entre suas Contas da AWS e VPCs. Certifique-se de que os intervalos de endereços IP de suas VPCs não se sobreponham aos intervalos de endereços IP de sua própria rede. Se você precisar de conectividade entre várias VPCs, você deve garantir que elas não tenham endereços IP sobrepostos.

O IP Address Manager (IPAM) facilita o planejamento, o rastreamento e o monitoramento dos endereços IP da sua aplicação. Para obter mais informações, consulte o Guia do IP Address Manager.

Selecione suas zonas de disponibilidade

Uma região da AWS é um local físico onde agrupamos data centers, conhecidos como zonas de disponibilidade. Cada zona de disponibilidade tem energia, resfriamento e segurança física independentes, com energia, redes e conectividade redundantes. As zonas de disponibilidade em uma região estão fisicamente separadas por uma distância significativa e interconectadas por meio de redes de alta largura de banda e baixa latência. É possível projetar sua aplicação para ser executada em várias zonas de disponibilidade para obter uma tolerância ainda maior a falhas.

Ambiente de produção

Para um ambiente de produção, recomendamos que você selecione pelo menos duas zonas de disponibilidade e implante seus recursos da AWS uniformemente em cada zona de disponibilidade ativa.

Ambientes de desenvolvimento ou teste

Para um ambiente de desenvolvimento ou teste, é possível optar por economizar dinheiro implantando seus recursos em apenas uma zona de disponibilidade.

Planeje sua conectividade com a Internet

Planeje dividir cada VPC em sub-redes com base em seus requisitos de conectividade. Por exemplo:

- Se você tiver servidores da Web que receberão tráfego de clientes na Internet, crie uma sub-rede para esses servidores em cada zona de disponibilidade.
- Se você também tiver servidores que receberão tráfego somente de outros servidores na VPC, crie uma sub-rede separada para esses servidores em cada zona de disponibilidade.
- Se você tiver servidores que receberão tráfego somente através de uma conexão de VPN para a sua rede, crie uma sub-rede separada para esses servidores em cada zona de disponibilidade.

Se a sua aplicação receberá tráfego da Internet, a VPC deverá ter um gateway da Internet. Anexar um gateway da Internet a uma VPC não faz com que suas instâncias sejam automaticamente acessíveis pela Internet. Além de anexar o gateway da Internet, você deve atualizar a tabela de rotas da sub-rede com uma rota para o gateway da Internet. As instâncias também devem ter endereços IP públicos e um grupo de segurança associado que permita o tráfego da Internet por meio de portas e protocolos específicos exigidos por sua aplicação.

Como alternativa, registre suas instâncias com um balanceador de carga voltado para a Internet. O balanceador de carga recebe tráfego dos clientes e o distribui pelas instâncias registradas em uma ou mais zonas de disponibilidade. Para obter mais informações, consulte Elastic Load Balancing. Para permitir que instâncias em uma sub-rede privada acessem a Internet (por exemplo, para baixar atualizações) sem permitir conexões de entrada não solicitadas da Internet, adicione um gateway NAT público em cada zona de disponibilidade ativa e atualize a tabela de rotas para enviar tráfego da Internet para o gateway NAT. Para ter mais informações, consulte the section called “Acessar a Internet a partir de uma sub-rede privada”.

Crie sua VPC

Depois de determinar o número de VPCs e sub-redes necessárias, quais blocos CIDR atribuir às suas VPCs e sub-redes e como conectar sua VPC à Internet, você estará pronto para criar sua VPC. Se você criar sua VPC usando o AWS Management Console e incluir sub-redes públicas em sua configuração, criaremos uma tabela de rotas para a sub-rede e adicionaremos as rotas necessárias

para o acesso direto à Internet. Para ter mais informações, consulte the section called “Crie uma VPC”.

Implantar a aplicação

Depois de ter criado a VPC, será possível implantar sua aplicação.

Ambiente de produção

Para um ambiente de produção, é possível usar um dos seguintes serviços para implantar servidores em várias zonas de disponibilidade, configurar a escalabilidade para manter o número mínimo de servidores exigido pela aplicação e registrar seus servidores com um balanceador de carga para distribuir o tráfego uniformemente entre os seus servidores.

- Amazon EC2 Auto Scaling
- EC2 Fleet
- Amazon Elastic Container Service (Amazon ECS)

Ambientes de desenvolvimento ou teste

Para um ambiente de desenvolvimento ou teste, é possível optar por executar uma única instância do EC2. Para obter mais informações, consulte Conceitos básicos do Amazon EC2 no Guia do usuário do Amazon EC2.

Endereçamento IP para suas VPCs e sub-redes

Os endereços IP habilitam recursos na sua VPC para se comunicar com outros e com recursos na Internet.

A notação Encaminhamento Entre Domínios Sem Classificação (CIDR) é uma forma de representar um endereço IP e sua máscara de rede. O formato desses endereços é:

- Um endereço IPv4 individual tem 32 bits, com quatro grupos de até três dígitos decimais. Por exemplo: 10.0.1.0.
- Um bloco CIDR IPv4 tem quatro grupos de até três dígitos decimais, 0-255, separados por pontos finais, seguidos por uma barra e um número de 0 a 32. Por exemplo, 10.0.0.0/16.
- Um endereço IPv6 individual tem 128 bits, com 8 grupos de 4 dígitos hexadecimais. Por exemplo: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.
- Um bloco CIDR IPv6 tem quatro grupos de até quatro dígitos hexadecimais, separados por caracteres de dois pontos, seguidos por dois caractere dois pontos, uma barra e um número de 1 a 128. Por exemplo: 2001:db8:1234:1a00::/56.

Para obter mais informações, consulte O que é CIDR?

Conteúdo

Endereços IPv4 privados

Endereços IPv4 privados (também chamados de endereços IP privados neste tópico) não são acessíveis pela Internet e podem ser usados para comunicação entre as instâncias na VPC. Ao iniciar uma instância em uma VPC, um endereço IP privado primário do intervalo de endereços IPv4 da sub-rede é atribuído à interface de rede primária (por exemplo, eth0) da instância. Cada instância também recebe um nome do host DNS privado (interno) que determina o endereço IP privado da instância. O nome do host pode ser de dois tipos: baseado em recursos ou baseado em IP. Para obter mais informações, consulte Nomeação de instâncias do EC2. Se você não especificar um endereço IP privado primário, selecionaremos um endereço IP disponível no intervalo da sub-rede. Para obter mais informações sobre interfaces de rede, consulte Interfaces de rede elástica no Guia do usuário do Amazon EC2.

Você pode atribuir endereços IP privados adicionais, conhecidos como endereços IP privados secundários, a instâncias que estejam sendo executadas em uma VPC. Ao contrário de um endereço IP privado primário, você poderá atribuir novamente um endereço IP privado secundário de uma interface de rede para outra. Um endereço IP privado permanece associado à interface de rede quando a instância é interrompida e reiniciada e é liberada quando a instância é terminada. Para obter mais informações sobre endereços IP primários e secundários, consulte Vários endereços IP no Guia do usuário do Amazon EC2.

Fazemos referência a endereços IP privados como os endereços IP que estão dentro do intervalo CIDR IPv4 da VPC. A maioria dos intervalos de endereço IP da VPC se enquadram nas escalas de endereços IP privados (não roteáveis publicamente) especificados no RFC 1918. No entanto, você pode usar blocos CIDR roteáveis publicamente para sua VPC. Independentemente do intervalo de endereço IP da VPC, não oferecemos suporte para acesso direto à Internet do bloco CIDR da VPC, incluindo um bloco CIDR publicamente roteável. É necessário configurar o acesso à Internet por meio de um gateway. Por exemplo, um gateway da Internet, um gateway privado virtual, uma conexão do AWS Site-to-Site VPN ou do AWS Direct Connect.

Nunca anunciamos o intervalo de endereços IPv4 de uma sub-rede na Internet.

Endereços IPv4 públicos

Todas as sub-redes têm um atributo que determina se uma interface de rede criada na sub-rede recebe automaticamente um endereço público IPv4 (também referido como um endereço IP público neste tópico). Dessa forma, ao iniciar uma instância em uma sub-rede com esse atributo habilitado, um endereço IP público é atribuído para a interface de rede primária criada para a instância. Um

endereço IP público é mapeado para o endereço IP privado primário pela tradução de endereço de rede (NAT).

> **Note**
>
> A AWS cobra por todos os endereços IPv4 públicos, incluindo endereços IPv4 públicos associados a instâncias em execução e endereços IP elásticos. Para obter mais informações, consulte a guia Endereço IPv4 público na página de preços da Amazon VPC.

Você pode controlar se sua instância recebe um endereço IP público fazendo o seguinte:

- Modificação do atributo de endereçamento IP público da sua sub-rede. Para obter mais informações, consulte Modificar os atributos de endereçamento IP da sua sub-rede.
- Habilitando ou desabilitando o recurso de endereçamento IP público durante a inicialização da instância, que substitui o atributo de endereçamento IP público da sub-rede.
- É possível cancelar a atribuição de um endereço IP público da sua instância após a execução gerenciando os endereços IP associados a uma interface de rede. Para obter mais informações, consulte Gerenciar endereços IP no Guia do usuário do Amazon EC2.

Um endereço IP público é atribuído do grupo da Amazon de endereços IP públicos; não está associado à sua conta. Quando um endereço IP público é desassociado de sua instância, ele é lançado de volta para o grupo e não está mais disponível para você usar. Em certos casos, liberamos o endereço IP público da instância ou atribuímos a ela um novo. Para obter mais informações, consulte Endereços IP públicos no Guia do usuário do Amazon EC2.

Se você precisar de um endereço IP público persistente alocado para sua conta, que pode ser atribuído e removido de instâncias conforme necessário, use um endereço IP elástico em vez disso. Para obter mais informações, consulte Associar endereços de IP elásticos a recursos em sua VPC.

Se sua VPC estiver ativada para oferecer suporte a nomes de host DNS, cada instância que recebe um endereço IP público ou um endereço IP elástico e um nome de host DNS público. Resolvemos um nome de host DNS público para o endereço IP público da instância fora da rede da instância e para o endereço IP privado da instância dentro da rede da instância. Para ter mais informações, consulte Atributos de DNS para sua VPC.

Caso esteja usando o Gerenciador de endereços IP (IPAM) da Amazon VPC, você pode obter um bloco contíguo de endereços IPv4 públicos da AWS e usá-lo para alocar endereços IP elásticos

sequenciais aos recursos da AWS. O uso de blocos de endereços IPv4 contíguos pode reduzir significativamente a sobrecarga de gerenciamento das listas de controle de acesso de segurança e simplificar a alocação e o rastreamento de endereços IP para empresas escalando na AWS. Para obter mais informações, consulte Allocate sequential Elastic IP addresses from an IPAM pool no Guia do usuário do IPAM da Amazon VPC.

Endereços IPv6

À medida que a Internet continua a crescer, também aumenta a necessidade de endereços IP. O formato mais comum para endereços IP é o IPv4. O novo formato para endereços IP é o IPv6, que fornece um espaço de endereçamento maior que o IPv4. O IPv6 resolve o problema de esgotamento do endereço IPv4 e permite que você conecte mais dispositivos à Internet. A transição é gradual, mas à medida que a adoção do IPv6 aumentar, você poderá simplificar suas redes e aproveitar os recursos avançados do IPv6 para melhorar a conectividade, a performance e a segurança.

Muitos serviços da AWS, como o Amazon EC2, o Amazon S3 e o Amazon CloudFront, são compatíveis com pilha dupla (IPv4 e IPv6) ou somente IPv6, o que permite que endereços IPv6 sejam atribuídos aos recursos e que eles sejam acessados pelo protocolo IPv6, e simplifica a configuração e o gerenciamento de rede para os clientes que adotam o IPv6. Outros serviços são compatíveis de modo limitado ou parcial com pilha dual e somente IPv6. Para obter mais informações sobre os serviços que são compatíveis com iPv6, consulte Serviços da AWS que oferecem suporte a IPv6.

Observe que alguns endereços IPv6 são reservados pela Internet Engineering Task Force. Para obter mais informações sobre intervalos de endereço IPv6 reservados, consulte Registro de endereço para finalidades especiais IANA IPv6 e RFC4291.

> **Note**
>
> O endereçamento IPv6 tanto público quanto privado está disponível na AWS. A AWS considera endereços IP públicos os que são anunciados na Internet pela AWS, enquanto os endereços IP privados não são e não podem ser anunciados na Internet pela AWS.

Conteúdo

Endereços IPv6 públicos

Os endereços IPv6 públicos são os endereços IPv6 que podem ser configurados para permanecer privados ou para ser acessados pela Internet.

Estas são algumas maneiras de você se preparar para usar endereços IPv6 públicos em suas workloads:

- Crie um IPAM com o Gerenciador de endereços IP da Amazon VPC e provisione um intervalo de endereços IPv6 públicos pertencente à Amazon para um grupo de endereços do IPAM. Para obter mais informações, consulte Criar grupos de IPv6 no Guia do usuário do IPAM da Amazon VPC.
- Se você tiver um IPAM e for proprietário de um intervalo de endereços IPv6 público, traga parte ou todo o intervalo de endereços IPv6 públicos para o IPAM, e provisione o intervalo de endereços IPv6 públicos para um grupo de endereços do IPAM. Para obter mais informações, consulte Tutorial: trazer seus endereços IP para o IPAM no Guia do usuário do IPAM da Amazon VPC.
- Se você não tiver um IPAM, mas for proprietário de um intervalo de endereços IPv6 públicos, traga parte ou todo o intervalo de endereços IPv6 públicos para a AWS. Para obter mais informações, consulte Traga seus próprios endereços IP (BYOIP) no Amazon EC2 no Guia do usuário do Amazon EC2.

Quando estiver pronto para usar endereços IPv6 públicos, você pode atribuí-los às instâncias (consulte Endereços IPv6 no Guia do usuário do Amazon EC2), alocar um bloco CIDR IPv6 público à sua VPC (consulte Adicionar ou remover um bloco CIDR da sua VPC) e associar o bloco CIDR IPv6 às suas sub-redes (consulte Modificar os atributos de endereçamento IP da sua sub-rede).

Endereços IPv6 privados

Endereços IPv6 privados são endereços IPv6 que não são anunciados e não podem ser anunciados na Internet pela AWS.

Você poderá usar endereços IPv6 privados se quiser que suas redes privadas sejam compatíveis com IPv6 e não tiver intenção de rotear o tráfego desses endereços para a Internet. Se você quiser se conectar à Internet em um recurso que tenha um endereço IPv6 privado, poderá fazê-lo, mas deverá rotear o tráfego por um recurso em outra sub-rede com um endereço IPv6 público para ter sucesso.

Há dois tipos de endereços IPv6 privados:

- Intervalos de ULAs IPv6: endereços IPv6 conforme definição da RFC4193. Esses intervalos de endereços sempre começam com “fc” ou “fd”, o que os torna facilmente identificáveis. Um espaço de ULAs IPv6 válido é todo espaço abaixo de fd00::/8 que não coincide com o intervalo reservado fd00: :/16 da Amazon.
- Intervalos de GUAs IPv6: endereços IPv6 conforme definição da RFC3587. A opção de usar intervalos de GUAs IPv6 como endereços IPv6 privados está desabilitada por padrão e deve ser habilitada para poder ser usada. Para obter mais informações, consulte Habilitar provisionamento de CIDRs de GUAs IPv6 no Guia do usuário do IPAM da Amazon VCP.

Observe o seguinte:

- Endereços IPv6 privados só estão disponíveis por meio do Gerenciador de endereços IP (IPAM) da Amazon VPC. O IPAM descobre recursos com endereços IPv6 ULA e GUA e monitora grupos em busca de espaços de endereços IPv6 ULA e GUA sobrepostos.
- Quando você usa intervalos de GUAs IPv6 privado, exigimos que use seus próprios intervalos de GUAs IPv6.
- Os endereços IPv6 privados não são e não podem ser anunciados na Internet pela AWS. A AWS não permite saída direta para a Internet pública de um intervalo IPv6 privado, mesmo que haja um gateway da internet ou um gateway da internet somente de saída na VPC. Os endereços IPv6 privados são automaticamente descartados na borda do gateway da Internet, garantindo que não sejam roteados publicamente.
- A AWS reserva os 4 primeiros e o último endereço IPv6 privado da sub-rede.
- Os intervalos válidos de ULAs IPv6 privados são de /9 a /60, a partir de fd80::/9.
- Se você tiver um intervalo de GUAs IPv6 privados alocado para uma VPC, não poderá usar um espaço de GUAs IPv6 públicos que coincida com espaço de GUAs que coincida com o espaço de GUAs iPv6 privados na mesma VPC.
- A comunicação entre recursos com intervalos de ULAs e GUAs IPv6 privados é compatível (por exemplo, por Direct Connect, emparelhamento de VPC, gateway de trânsito e conexões de VPN).
- Você pode usar endereços IPv6 privados com sub-redes da VPC somente IPv6 e de pilha dupla, balanceadores de carga elásticos e endpoints do AWS Global Accelerator.
- Endereços IPv6 privados não são cobrados.

Estas são algumas maneiras de você se preparar para usar endereços IPv6 privados em suas workloads:

- Crie um IPAM com o Gerenciador de endereços IP da Amazon VPC e provisione um intervalo de ULAs IPv6 privados para um grupo de endereços do IPAM. Para obter mais informações, consulte Criar grupos de IPv6 no Guia do usuário do IPAM da Amazon VPC.
- Crie um IPAM com o Gerenciador de endereços IP da Amazon VPC e provisione um intervalo de GUAs IPv6 privado para um grupo de endereços do IPAM. A opção de usar intervalos de GUAs IPv6 como endereços IPv6 privados está desabilitada por padrão e deve ser habilitada no IPAM para poder ser usada. Para obter mais informações, consulte Habilitar provisionamento de CIDRs de GUAs IPv6 no Guia do usuário do IPAM da Amazon VCP.

Quando estiver pronto para usar endereços IPv6 privados, você poderá alocar um bloco CIDR IPv6 privado de um grupo do IPAM para sua VPC (consulte Adicionar ou remover um bloco CIDR da sua VPC) e associar o bloco CIDR IPv6 às suas sub-redes (consulte Modificar os atributos de endereçamento IP da sua sub-rede).

Use seus próprios endereços IP

É possível trazer todo ou parte do seu próprio intervalo público de endereços IPv4 ou intervalo de endereços IPv6 para sua conta da AWS. Você continua a ter o intervalo de endereços, mas a AWS o anuncia na Internet por padrão. Depois de levar o intervalo de endereços para a AWS, ele aparece em sua conta como um grupo de endereços. É possível criar um endereço IP elástico pelo grupo de endereços IPv4 e associar um bloco CIDR IPv6 do grupo de endereços IPv6 a uma VPC.

Para obter mais informações, consulte Traga seus próprios endereços IP (BYOIP) no Guia do usuário do Amazon EC2.

Use o IP Address Manager da Amazon VPC

O IP Address Manager da Amazon VPC (IPAM) é um recurso da VPC que facilita o planejamento, o rastreamento e o monitoramento de endereços IP de suas workloads da AWS. É possível usar o IPAM para alocar CIDRs de endereço IP para VPCs usando regras de negócios específicas.

Para mais informações, consulte What is IPAM? (O que é IPAM?) no Guia do usuário do Amazon VPC IPAM.

Blocos CIDR da VPC

Os endereços IP da sua nuvem privada virtual (VPC) são representados usando a notação Encaminhamento Entre Domínios Sem Classificação (CIDR). Uma VPC deve ter um bloco CIDR IPv4 associado. Opcionalmente, é possível associar blocos CIDR IPv4 e um ou mais blocos CIDR IPv6. Para ter mais informações, consulte Endereçamento IP para suas VPCs e sub-redes.

Conteúdo

Blocos CIDR IPv4 da VPC

Ao criar uma VPC, você deve especificar um bloco CIDR IPv4 para a VPC. O tamanho permitido para o bloco é entre uma máscara de rede `/16` (65.536 endereços IP) e uma máscara de rede `/28` (16 endereços IP). Depois de criar a VPC, você pode associar blocos CIDR IPv4 adicionais à VPC. Para ter mais informações, consulte Adicionar ou remover um bloco CIDR da sua VPC.

Quando você cria uma VPC, é recomendável especificar um bloco CIDR dos intervalos de endereços IPv4 privados conforme especificado em RFC 1918:

Intervalo do RFC 1918	Bloco CIDR de exemplo
10.0.0.0 - 10.255.255.255 (prefixo 10/8)	10.0.0.0/16
172.16.0.0 - 172.31.255.255 (prefixo 172.16/12)	172.31.0.0/16
192.168.0.0 - 192.168.255.255 (prefixo 192.168/16)	192.168.0.0/20

> **Important**
>
> Determinados serviços da AWS fazem uso dos intervalos CIDR `172.17.0.0/16` e `172.16.0.0/12`. Os serviços podem enfrentar conflitos de endereço IP se os intervalos de endereços IP já estiverem em uso em qualquer parte da sua rede. Por exemplo, o AWS Cloud9 e o Amazon SageMaker AI usam `172.17.0.0/16` e o Amazon RDS usa `172.16.0.0/12`. Para evitar conflitos, não use esses intervalos ao criar sua VPC. Para obter mais informações, consulte Não é possível se conectar ao ambiente do EC2 porque os endereços IP da VPC são usados pelo Docker no Guia do usuário do AWS Cloud9.

É possível criar uma VPC com um bloco CIDR publicamente roteável que esteja fora dos intervalos de endereços IPv4 privados especificados na RFC 1918. No entanto, para fins dessa documentação, referimo-nos aos endereços IP privados como os endereços IPv4 que estão no intervalo CIDR da VPC.

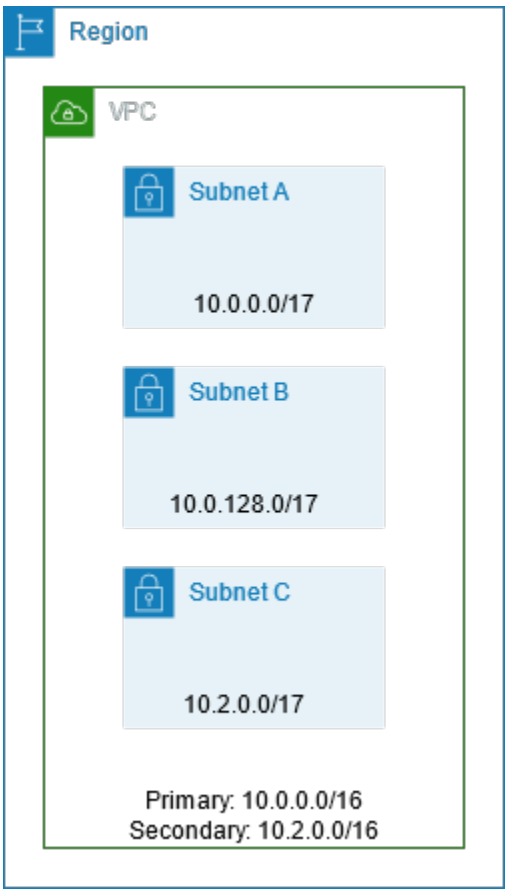
Ao criar uma VPC para uso com um serviço da AWS, verifique a documentação do serviço em busca de requisitos específicos para sua configuração.

Se você criar uma VPC usando uma ferramenta da linha de comando ou a API do Amazon EC2, o bloco CIDR será automaticamente modificado para sua forma canônica. Por exemplo, se você especificar 100.68.0.18/18 para o bloco CIDR, criaremos um bloco CIDR de 100.68.0.0/18.

Gerencie blocos CIDR IPv4 para uma VPC

Você pode associar blocos CIDR IPv4 secundários à VPC. Quando você associa um bloco CIDR à VPC, uma rota é adicionada automaticamente às tabelas de rotas da VPC para habilitar o roteamento na VPC (o destino é o bloco CIDR e o alvo é `local`).

No exemplo a seguir, a VPC tem um bloco CIDR principal e um bloco CIDR secundário. Os blocos CIDR para a sub-rede A e a sub-rede B são do bloco CIDR principal da VPC. O bloco CIDR para a sub-rede C é do bloco CIDR secundário da VPC.



A tabela de rotas a seguir mostra as rotas locais para a VPC.

Destino	Destino
10.0.0.0/16	Local
10.2.0.0/16	Local

Para adicionar um bloco CIDR à VPC, as seguintes regras devem ser aplicadas:

- O tamanho do bloco permitido é entre uma máscara de rede `/28` e máscara de rede `/16`.
- O bloco CIDR não deve sobrepor nenhum bloco CIDR existente que esteja associado à VPC.
- Há restrições nos intervalos de endereços IPv4 que você pode usar. Para obter mais informações, consulte Restrições de associação de bloco CIDR IPv4.
- Não é possível aumentar ou diminuir o tamanho de um bloco CIDR existente.

- Você tem uma cota no número de blocos CIDR que pode associar a uma VPC e ao número de rotas que pode adicionar a uma tabela de rotas. Não será possível associar um bloco CIDR se suas cotas forem excedidas por causa disso. Para obter mais informações, consulte Cotas da Amazon VPC.
- O bloco CIDR não deve ser igual nem maior que um intervalo CIDR de destino em uma rota em nenhuma das tabelas de rotas da VPC. Por exemplo, em uma VPC na qual o bloco CIDR primário é `10.2.0.0/16`, você tem uma rota existente em uma tabela de rotas com um destino de `10.0.0.0/24` para um gateway privado virtual. Você deseja associar um bloco CIDR secundário no intervalo `10.0.0.0/16`. Devido à rota existente, não é possível associar um bloco CIDR de `10.0.0.0/24` ou maior. No entanto, é possível associar um bloco CIDR secundário de `10.0.0.0/25` ou menor.
- As seguintes regras se aplicam quando você adiciona blocos CIDR IPv4 a uma VPC que faz parte de uma conexão de emparelhamento de VPC:
  - Se a conexão de emparelhamento da VPC for `active`, você poderá adicionar blocos CIDR a uma VPC desde que eles não sobreponham um bloco CIDR da VPC par.
  - Se a conexão de emparelhamento da VPC for `pending-acceptance`, o proprietário da VPC solicitante não poderá adicionar nenhum bloco CIDR à VPC, independentemente de ele sobrepor o bloco CIDR da VPC receptora. O proprietário da VPC receptora deve aceitar a conexão de emparelhamento, ou o proprietário da VPC solicitante deve excluir a solicitação da conexão de emparelhamento de VPC, adicionar o bloco CIDR e, em seguida, solicitar uma nova conexão de emparelhamento de VPC.
  - Se a conexão de emparelhamento da VPC for `pending-acceptance`, o proprietário da VPC solicitante poderá adicionar blocos CIDR à VPC. Se um bloco CIDR secundário for sobreposto por um bloco CIDR da VPC solicitante, a solicitação da conexão de emparelhamento da VPC falhará e não poderá ser aceita.
- Se você estiver usando o AWS Direct Connect para se conectar a várias VPCs por um gateway do Direct Connect, as VPCs associadas ao gateway do Direct Connect não deverão ter blocos CIDR sobrepostos. Se você adicionar um bloco CIDR a uma das VPCs associadas ao gateway do Direct Connect, certifique-se de que o novo bloco CIDR não se sobreponha ao bloco CIDR existente de nenhuma outra VPC associada. Para obter mais informações, consulte Gateways do Direct Connect no Manual do usuário do AWS Direct Connect.
- Ao adicionar ou remover um bloco CIDR, ele pode passar por vários estados: `associating` | `associated` | `disassociating` | `disassociated` | `failing` | `failed`. O bloco CIDR está pronto para uso quando está no estado `associated`.

Você pode desassociar um bloco CIDR que associou à VPC. No entanto, você não pode desassociar o bloco CIDR com o qual você criou a VPC originalmente (o bloco CIDR principal). Para visualizar o CIDR primário da sua VPC no console da Amazon VPC, escolha Your VPCs (Suas VPCs), selecione a caixa de seleção para a sua VPC e escolha a guia CIDRs (CIDRs). Para visualizar o CIDR primário usando a AWS CLI, use o comando describe-vpcs (Descrever VPCs) da seguinte forma. O CIDR primário é retornado ao `CidrBlock element` de nível superior.

```
aws ec2 describe-vpcs --vpc-id vpc-1a2b3c4d --query Vpcs[*].CidrBlock --output text
```

O seguinte é um exemplo de saída.

```
10.0.0.0/16
```

Restrições de associação de bloco CIDR IPv4

A tabela a seguir dá uma visão geral das associações de bloco CIDR de VPC permitidas e restritas. O motivo das restrições é que alguns serviços da AWS usam recursos entre VPCs e entre contas que exigem blocos CIDR não conflitantes no lado do serviço da AWS.

Intervalo de endereços IP	Associações restritas	Associações permitidas
10.0.0.0/8	Blocos CIDR de outros intervalos RFC 1918* (172.16.0.0/12 e 192.168.0.0/16). Se qualquer um dos blocos CIDR associados à VPC for do intervalo 10.0.0.0/15 (10.0.0.0 a 10.1.255.255), você não poderá adicionar um bloco CIDR do intervalo 10.0.0.0/16 (10.0.0.0 a 10.0.255.255). Blocos CIDR do intervalo 198.19.0.0/16.	Qualquer outro bloco CIDR no intervalo 10.0.0.0/8 entre uma máscara de rede /16 e uma máscara de rede /28 que não seja restrita. Qualquer bloco CIDR IPv4 publicamente roteável (não RFC 1918) entre uma máscara de rede /16 e uma máscara de rede /28 ou um bloco de CIDR entre uma máscara de rede /16 e uma máscara de rede /28 do intervalo 100.64.0.0/10.
169.254.0.0/16	Os blocos CIDR do bloco "link local" são reservados conforme descrito na	

Intervalo de endereços IP	Associações restritas	Associações permitidas
	RFC 5735 e não podem ser atribuídos a VPCs.	
172.16.0.0/12	Blocos CIDR de outros intervalos RFC 1918* (10.0.0.0/8 e 192.168.0.0/16). Bloco CIDR do intervalo 172.31.0.0/16. Blocos CIDR do intervalo 198.19.0.0/16.	Qualquer outro bloco CIDR no intervalo 172.16.0.0/12 entre uma máscara de rede /16 e uma máscara de rede /28 que não seja restrita. Qualquer bloco CIDR IPv4 publicamente roteável (não RFC 1918) entre uma máscara de rede /16 e uma máscara de rede /28 ou um bloco de CIDR entre uma máscara de rede /16 e uma máscara de rede /28 do intervalo 100.64.0.0/10.
192.168.0.0/16	Blocos CIDR de outros intervalos RFC 1918* (10.0.0.0/8 and 172.16.0.0/12). Blocos CIDR do intervalo 198.19.0.0/16.	Qualquer outro bloco CIDR no intervalo 192.168.0.0 entre uma máscara de rede /16 e uma máscara de rede /28. Qualquer bloco CIDR IPv4 publicamente roteável (não RFC 1918) entre uma máscara de rede /16 e uma máscara de rede /28 ou um bloco CIDR do intervalo 100.64.0.0/10 entre uma máscara de rede /16 e uma máscara de rede /28.

Intervalo de endereços IP	Associações restritas	Associações permitidas
198.19.0.0/16	Blocos CIDR dos intervalos RFC 1918*.	Qualquer bloco CIDR IPv4 publicamente roteável (não RFC 1918) entre uma máscara de rede /16 e uma máscara de rede /28 ou um bloco CIDR do intervalo 100.64.0.0/10 entre uma máscara de rede /16 e uma máscara de rede /28.
Bloco CIDR encaminhado publicamente (não RFC 1918) ou um bloco CIDR do intervalo 100.64.0.0/10	Blocos CIDR dos intervalos RFC 1918*. Blocos CIDR do intervalo 198.19.0.0/16.	Qualquer outro bloco CIDR IPv4 publicamente roteável (não RFC 1918) entre uma máscara de rede /16 e uma máscara de rede /28 ou um bloco de CIDR entre uma máscara de rede /16 e uma máscara de rede /28 do intervalo 100.64.0.0/10. Além disso, é possível associar um CIDR em um dos intervalos RFC 1918, mas para fazer isso, é necessário, primeiro, adicionar esse CIDR ao criar a VPC e, em seguida, adicionar o CIDR que não pertence ao intervalo RFC 1918.

Os intervalos *RFC 1918 são os intervalos de endereços IPv4 privados especificados no RFC 1918.

Blocos CIDR IPv6 da VPC

Você pode associar um único bloco CIDR IPv6 ao criar uma nova VPC ou pode associar até cinco blocos CIDR IPv6 de a `/44` em `/60` incrementos de `/4`. É possível solicitar um bloco CIDR IPv6 do grupo de endereços IPv6 da Amazon. Para ter mais informações, consulte Adicionar ou remover um bloco CIDR da sua VPC.

Se você associou um bloco CIDR IPv6 à sua VPC, pode associar um bloco CIDR IPv6 a uma sub-rede existente na sua VPC ou ao criar uma nova sub-rede. Para ter mais informações, consulte the section called “Dimensionamento da sub-rede para IPv6”.

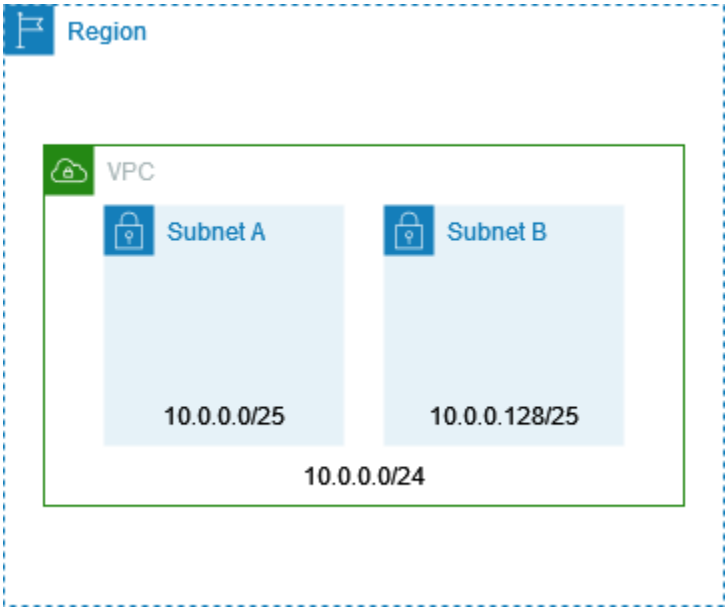
Por exemplo, você cria uma VPC e especifica que deseja associar um bloco CIDR IPv6 fornecido pela Amazon à VPC. A Amazon atribui o seguinte bloco CIDR IPv6 a sua VPC: `2001:db8:1234:1a00::/56`. Não é possível escolher o intervalo de endereços IP por conta própria. Você pode criar uma sub-rede e associar um bloco CIDR IPv6 deste intervalo; por exemplo, `2001:db8:1234:1a00::/64`.

É possível desassociar um bloco CIDR IPv6 de uma VPC. Depois de ter desassociado um bloco CIDR IPv6 de uma VPC, você não poderá esperar receber o mesmo CIDR se você associar um bloco CIDR IPv6 com sua VPC novamente mais tarde.

Blocos CIDR de sub-redes

Os endereços IP das sub-redes são representados usando a notação Encaminhamento Entre Domínios Sem Classificação (CIDR). O bloco CIDR de uma sub-rede pode ser igual ao bloco CIDR da VPC (para criar uma única sub-rede na VPC) ou um subconjunto do bloco CIDR para a VPC (para criar várias sub-redes na VPC). Se você criar mais de uma sub-rede em uma VPC, os blocos CIDR das sub-redes não podem se sobrepor.

Por exemplo, se você criar uma VPC com o bloco CIDR `10.0.0.0/24`, ela oferece suporte a 256 endereços IP. Você pode quebrar esse bloco CIDR em duas sub-redes, cada um oferecendo suporte a 128 endereços IP. Uma sub-rede usa o bloco CIDR `10.0.0.0/25` (para endereços `10.0.0.0` - `10.0.0.127`) e o outro usa o bloco CIDR `10.0.0.128/25` (para endereços `10.0.0.128` - `10.0.0.255`).



Existem ferramentas online que podem auxiliá-lo no cálculo e na criação de blocos CIDR para sub-redes IPv4 e IPv6. É possível encontrar ferramentas que se adequam às suas necessidades procurando termos como “calculadora de sub-rede” ou “calculadora de CIDR”. Seu grupo de engenharia de rede pode oferecer suporte na determinação dos blocos CIDR IPv4 e IPv6 adequados para suas sub-redes.

Dimensionamento da sub-rede para IPv4

O tamanho permitido para um bloco CIDR IPv4 de sub-rede varia entre uma máscara de rede `/28` e outra máscara de rede `/16`. Os quatro primeiros endereços IP e o último endereço IP em cada bloco CIDR de sub-rede não estão disponíveis para você usar e não podem ser atribuídos a um recurso, p. ex., a uma instância do EC2. Por exemplo, em uma sub-rede com bloco CIDR `10.0.0.0/24`, os seguintes cinco endereços IP são reservados:

- 10.0.0.0: endereço de rede.
- 10.0.0.1: reservado pela AWS para o roteador da VPC.
- 10.0.0.2: reservado pela AWS. O endereço IP do servidor de DNS é a base do intervalo de rede da VPC mais dois. Para VPCs com vários blocos CIDR, o endereço IP de servidor de DNS está localizado no CIDR principal. Também reservamos a base de cada intervalo de sub-rede mais dois para todos os blocos CIDR na VPC. Para ter mais informações, consulte Servidor de DNS da Amazon.
- 10.0.0.3: reservado pela AWS para uso futuro.

- 10.0.0.255: endereço de transmissão de rede. Não oferecemos suporte para transmissão em uma VPC, portanto, reservamos este endereço.

Se você criar uma sub-rede usando uma ferramenta da linha de comando ou a API do Amazon EC2, o bloco CIDR será automaticamente modificado para sua forma canônica. Por exemplo, se você especificar 100.68.0.18/18 para o bloco CIDR, criaremos um bloco CIDR de 100.68.0.0/18.

Se você trouxer um intervalo de endereços IPv4 para a AWS usando BYOIP, poderá usar todos os endereços IP do intervalo, incluindo o primeiro endereço (o endereço de rede) e o último endereço (o endereço de broadcast).

Dimensionamento da sub-rede para IPv6

Se você associou um bloco CIDR IPv6 a sua VPC, é possível associar um bloco CIDR IPv6 a uma sub-rede existente na sua VPC ou ao criar uma nova sub-rede. Os possíveis comprimentos da máscara de rede IPv6 estão entre `/44` e `/64` em incrementos de `/4`.

Existem ferramentas disponíveis na Internet que ajudam a calcular e criar blocos CIDR de sub-rede IPv6. É possível encontrar outras ferramentas que se adequam às suas necessidades procurando termos como “calculadora de sub-rede IPv6” ou “calculadora de CIDR IPv6”. O grupo de engenharia de rede também pode ajudar a determinar os blocos CIDR IPv6 para especificar as sub-redes.

Os quatro primeiros endereços IPv6 e o último endereço IPv6 em cada bloco CIDR de sub-rede não estão disponíveis para você usar e não podem ser atribuídos a uma instância do EC2. Por exemplo, em uma sub-rede com bloco CIDR `2001:db8:1234:1a00/64`, os seguintes cinco endereços IP são reservados:

- `2001:db8:1234:1a00::`
- `2001:db8:1234:1a00::1`: Reservado pela AWS para o roteador da VPC.
- `2001:db8:1234:1a00::2`
- `2001:db8:1234:1a00::3`
- `2001:db8:1234:1a00:ffff:ffff:ffff:ffff`

Além do endereço IP reservado pela AWS para o roteador da VPC no exemplo acima, os endereços IPv6 a seguir são reservados para o roteador da VPC padrão.

- Um endereço IPv6 de local de link no intervalo FE80::/10 gerado usando EUI-64. Para obter mais informações sobre endereços locais de link, consulte Endereço local de link.

- O endereço IPv6 local de link `FE80:ec2::1`.

Se precisar se comunicar com o roteador VPC via IPv6, você pode configurar seus aplicativos para se comunicarem com o endereço que melhor atenda às suas necessidades.

Comparar IPv4 e IPv6

A tabela a seguir resume as diferenças entre IPv4 e IPv6 no Amazon EC2 e na Amazon VPC. Para obter uma lista de serviços da AWS compatíveis com configuração de pilha dupla (IPv4 e IPv6) e configurações somente Pv6, consulte Serviços que oferecem suporte a IPv6.

Característica	IPv4	IPv6
Tamanho da VPC	Até 5 CIDRs de /16 a /28. Essa cota é ajustável.	Até 5 CIDRs de /44 a /60 em incrementos de /4. Essa cota é ajustável.
Tamanho da sub-rede	De /16 a /28	De /44 a /64 em incrementos de /4.
Seleção de endereço	Você pode escolher o bloco CIDR IPv4 para sua VPC ou alocar um bloco CIDR do Amazon VPC IP Address Manager (IPAM). Para mais informações, consulte What is IPAM? (O que é IPAM?) no Guia do usuário do Amazon VPC IPAM.	Você pode trazer seu próprio bloco CIDR IPv6 para sua VPC na AWS, escolher um bloco CIDR IPv6 fornecido pela Amazon ou alocar um bloco CIDR do Amazon VPC IP Address Manager (IPAM). Para mais informações, consulte What is IPAM? (O que é IPAM?) no Guia do usuário do Amazon VPC IPAM.
Acesso à Internet	Requer um gateway da Internet.	Requer um gateway da Internet. Suporta comunicação somente de saída usando um gateway da Internet somente de saída.
Endereços IP elásticos	Compatível. Fornece a uma instância do EC2 um endereço IPv4 público estático.	Sem compatibilidade. Os EIPs mantêm o endereço IPv4 público de uma instância estático na reinicial

Característica	IPv4	IPv6
		ização da instância. Os endereços IPv6 são estáticos por padrão.
Gateways NAT	Compatível. As instâncias em sub-redes privadas podem se conectar à Internet usando um gateway NAT público ou a recursos em outras VPCs usando um gateway NAT privado.	Compatível. Você pode usar um gateway NAT com NAT64 para habilitar a comunicação de instância s em sub-redes somente IPv6 com recursos somente IPv4 nas VPCs, em suas redes on-premises ou pela Internet.
Nomes de DNS	As instâncias recebem um IPBN fornecido pela Amazon ou nomes de DNS baseados em RBN. O nome DNS determina os registros DNS selecionados para a instância.	A instância recebe um IPBN fornecido pela Amazon ou nomes de DNS baseados em RBN. O nome DNS determina os registros DNS selecionados para a instância.

Consolide e gerencie blocos CIDR de rede com listas de prefixos gerenciadas

Uma lista de prefixos gerenciados é um conjunto de um ou mais blocos CIDR. Você pode usar listas de prefixos para facilitar a configuração e a manutenção de grupos de segurança e tabelas de rotas. Você pode criar uma lista de prefixos a partir dos endereços IP usados com frequência e referenciá-los como um conjunto em regras e rotas no grupo de segurança em vez de referenciá-los individualmente. Por exemplo, você pode consolidar regras do grupo de segurança com diferentes blocos CIDR, mas a mesma porta e protocolo em uma única regra que usa uma lista de prefixos. Se você escalar a rede e precisar permitir tráfego de outro bloco CIDR, poderá atualizar a lista de prefixos relevante e todos os grupos de segurança que usam a lista de prefixos serão atualizados. Você também pode usar listas de prefixos gerenciadas com outras contas da AWS usando o Resource Access Manager (RAM).

Existem dois tipos de listas de prefixos:

- Listas de prefixos gerenciadas pelo cliente — Conjuntos de intervalos de endereços IP que você define e gerencia. Você pode compartilhar sua lista de prefixos com outras contas da AWS, o que permite que essas contas façam referência à lista de prefixos em seus próprios recursos.
- Listas de prefixos gerenciados pela AWS: conjuntos de intervalos de endereços IP para serviços da AWS. Não é possível criar, modificar, compartilhar ou excluir uma lista de prefixos gerenciados pela AWS.

Tópicos

Conceitos e regras das listas de prefixos

Uma lista de prefixos consiste em entradas. Cada entrada consiste em um bloco CIDR e, opcionalmente, uma descrição para o bloco CIDR.

Listas de prefixos gerenciadas pelo cliente

As regras a seguir se aplicam às listas de prefixos gerenciados pelo cliente:

- Uma lista de prefixos é compatível com um único tipo de endereçamento IP (IPv4 ou IPv6). Não é possível combinar blocos CIDR IPv4 e IPv6 em uma única lista de prefixos.
- Uma lista de prefixos se aplica somente à região em que você a criou.
- Ao criar uma lista de prefixos, você deve especificar o número máximo de entradas com as quais a lista de prefixos é compatível.
- Quando você faz referência a uma lista de prefixos em um recurso, o número máximo de entradas para as listas de prefixos é considerado como parte da cota para o número de entradas para o recurso. Por exemplo, se você cria uma lista de prefixos com o máximo de 20 entradas e faz referência a essa lista de prefixos em uma regra do grupo de segurança, isso contará como 20 regras para o grupo de segurança.

- Quando você faz referência a uma lista de prefixos em uma tabela de rotas, as regras de prioridade da rota se aplicam. Para ter mais informações, consulte Prioridade de rotas para listas de prefixos.
- Você pode modificar uma lista de prefixos. Quando você adiciona ou remove entradas de uma lista de prefixos, criamos uma nova versão da lista de prefixos. Os recursos que fazem referência ao prefixo sempre usam a versão atual (mais recente). Você pode restaurar as entradas de uma versão anterior da lista de prefixos, o que também cria uma nova versão.
- Há cotas relacionadas a listas de prefixos. Para ter mais informações, consulte Listas de prefixos gerenciadas pelo cliente.
- As listas de prefixos gerenciadas pelo cliente estão disponíveis em todas as Regiões comerciais da AWS (incluindo as regiões GovCloud (EUA) e China).

Listas de prefixos gerenciados pela AWS

As seguintes regras aplicam-se a listas de prefixos gerenciados pela AWS:

- Não é possível criar, modificar, compartilhar ou excluir uma lista de prefixos gerenciados pela AWS.
- Diferentes listas de prefixos gerenciados pela AWS têm um peso diferente quando você as usa. Para ter mais informações, consulte Peso da lista de prefixos gerenciados pela AWS.
- Não é possível visualizar o número de versão de uma lista de prefixos gerenciados pela AWS.

Identity and Access Management para as listas de prefixos

Por padrão, os usuários do não têm permissão para criar, visualizar, modificar ou excluir listas de prefixos. É possível criar uma política do IAM e anexá-la a um perfil que permita que os usuários trabalhem com listas de prefixos.

Para obter uma lista de ações da Amazon VPC e dos recursos e chaves de condição que você pode usar em uma política do IAM, consulte Actions, resources, and condition keys for Amazon EC2 na Referência de autorização do serviço.

O exemplo de política a seguir permite que os usuários visualizem e trabalhem somente com listas de prefixos `pl-123456abcde123456`. Os usuários não podem criar ou excluir listas de prefixos.

```
{
   "Version": "2012-10-17",
```

```
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:GetManagedPrefixListAssociations",
        "ec2:GetManagedPrefixListEntries",
        "ec2:ModifyManagedPrefixList",
        "ec2:RestoreManagedPrefixListVersion"
      ],
      "Resource": "arn:aws:ec2:region:account:prefix-list/pl-123456abcde123456"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeManagedPrefixLists",
      "Resource": "*"
    }
   ]
}
```

Para obter mais informações sobre como trabalhar com o IAM na Amazon VPC, consulte Identity and Access Management para o Amazon VPC.

Listas de prefixos gerenciadas pelo cliente

As listas de prefixos gerenciadas pelo cliente permitem a você definir e manter seus próprios conjuntos de intervalos de endereços IP, conhecidos como prefixos, na AWS. Em vez de codificar esses endereços IP em seus vários recursos, você pode criar uma lista de prefixos centralizada e fazer referência a ela sempre que necessário. Isso não apenas simplifica o gerenciamento de seus endereços IP, mas também promove consistência e reutilização em todo o seu cenário da AWS.

Um dos recursos de destaque das listas de prefixos gerenciadas pelo cliente é a capacidade de compartilhá-las com outras contas da AWS. Ao conceder acesso às suas listas de prefixos, você pode permitir que outras equipes ou organizações aproveitem seus intervalos de endereços IP definidos em seus próprios recursos. Essa abordagem colaborativa promove uma experiência de nuvem mais coesa e eficiente na qual o gerenciamento de endereços IP é compartilhado e sincronizado.

Nas seções a seguir, vamos nos aprofundar nos aspectos práticos de trabalhar com listas de prefixos gerenciadas pelo cliente, incluindo orientações passo a passo sobre como criar, gerenciar e compartilhar seus intervalos de endereços IP.

Tarefas

Trabalhar com as listas de prefixos gerenciadas pelo cliente

Esta seção descreve como trabalhar com listas de prefixos gerenciadas pelo cliente.

Conteúdo

Criar uma lista de prefixos

Ao criar uma lista de prefixos, você deve especificar o número máximo de entradas com as quais a lista de prefixos é compatível.

Limitação

Você não pode adicionar uma lista de prefixos a uma regra do grupo de segurança se o número de regras mais o máximo de entradas para a lista de prefixos exceder a cota de regras por grupo de segurança para a conta.

Como criar uma lista de prefixos usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Listas de prefixos gerenciados.
3. Escolha Criar lista de prefixos.
4. Em Nome da lista de prefixos, insira um nome para a lista de prefixos.
5. Em Máximo de entradas, insira o número máximo de entradas para a lista de prefixos.

6. Em Família de endereços, indique se a lista de prefixos é compatível com entradas IPv4 ou IPv6.
7. Em Entradas da lista de prefixos, escolha Adicionar nova entrada e insira o bloco CIDR e uma descrição para a entrada. Repita esta etapa para cada entrada.
8. (Opcional) Em Tags, adicione tags à lista de prefixos para ajudá-lo a identificá-la posteriormente.
9. Escolha Criar lista de prefixos.

Como criar uma lista de prefixos usando a AWS CLI

Use o comando create-managed-prefix-list.

Visualizar listas de prefixos

Você pode visualizar listas de prefixos, listas de prefixos compartilhadas com você e listas de prefixos gerenciadas pela AWS.

Como visualizar listas de prefixos usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Listas de prefixos gerenciados.
3. A coluna ID do proprietário mostra o ID de conta da AWS do proprietário da lista de prefixos. Para listas de prefixos gerenciados pela AWS, o Owner ID (ID do proprietário) é AWS.

Como visualizar listas de prefixos usando a AWS CLI

Use o comando describe-managed-prefix-lists.

Visualizar as entradas de uma lista de prefixos

Você pode visualizar as entradas das suas listas de prefixos, listas de prefixos compartilhadas com você e listas de prefixos gerenciadas pela AWS.

Como visualizar as entradas de uma lista de prefixos usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Listas de prefixos gerenciados.
3. Marque a caixa de seleção da lista de prefixos.
4. No painel inferior, escolha Entradas para visualizar as entradas da lista de prefixos.

Como visualizar as entradas de uma lista de prefixos usando a AWS CLI

Use o comando get-managed-prefix-list-entries.

Visualizar associações (referências) para a lista de prefixos

Você pode visualizar os IDs e proprietários dos recursos associados à lista de prefixos. Os recursos associados são recursos que fazem referência à lista de prefixos nas entradas ou regras.

Limitação

Não é possível visualizar recursos associados para uma lista de prefixos gerenciados pela AWS.

Como visualizar associações de listas de prefixos usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Listas de prefixos gerenciados.
3. Marque a caixa de seleção da lista de prefixos.
4. No painel inferior, escolha Associações para visualizar os recursos que fazem referência à lista de prefixos.

Como visualizar associações de listas de prefixos usando a AWS CLI

Use o comando get-managed-prefix-list-associations.

Modificar uma lista de prefixos

É possível modificar o nome da sua lista de prefixos e adicionar ou remover entradas. Para modificar o número máximo de entradas, consulte Redimensionar uma lista de prefixos.

Atualizar as entradas de uma lista de prefixos cria uma nova versão da lista de prefixos. Atualizar o nome ou o número máximo de entradas de uma lista de prefixos não cria uma nova versão da lista de prefixos.

Considerações

- Não é possível modificar uma lista de prefixos gerenciados pela AWS.
- Quando você aumenta o número máximo de entradas em uma lista de prefixos, o tamanho máximo aumentado é aplicado à cota de entradas para os recursos que fazem referência à lista

de prefixos. Se qualquer um desses recursos não for capaz de suportar o tamanho máximo aumentado, a operação de modificação falhará e o tamanho máximo anterior será restaurado.

Como modificar uma lista de prefixos usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Listas de prefixos gerenciados.
3. Marque a caixa de seleção da lista de prefixos e escolha Actions (Ações), Modify prefix list (Modificar lista de prefixos).
4. Em Nome da lista de prefixos, insira um novo nome para a lista de prefixos.
5. Em Entradas da lista de prefixos, escolha Remover para remover uma entrada existente. Para adicionar uma nova entrada, escolha Adicionar nova entrada e insira o bloco CIDR e uma descrição para a entrada.
6. Escolha Salvar lista de prefixos.

Como modificar uma lista de prefixos usando a AWS CLI

Use o comando modify-managed-prefix-list.

Redimensionar uma lista de prefixos

É possível redimensionar uma lista de prefixos e modificar o número máximo de entradas da lista de prefixos até 1000. Para obter mais informações sobre cotas de listas de prefixos gerenciadas pelo, consulte Listas de prefixos gerenciadas pelo cliente.

Para redimensionar uma lista de prefixos usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Listas de prefixos gerenciados.
3. Marque a caixa de seleção da lista de prefixos e escolha Actions (Ações), Resize prefix list (Redimensionar lista de prefixos).
4. Em New max entries (Novo valor máximo de entradas), insira um valor.
5. Selecione Resize (Redimensionar).

Para redimensionar uma lista de prefixos usando a AWS CLI

Use o comando modify-managed-prefix-list.

Restaurar uma versão anterior de uma lista de prefixos

Você pode restaurar as entradas de uma versão anterior da sua lista de prefixos. Isso cria uma nova versão da lista de prefixos.

Se você diminuiu o tamanho da lista de prefixos, deve garantir que a lista de prefixos seja grande o suficiente para conter as entradas da versão anterior.

Como restaurar uma versão anterior de lista de prefixos usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Listas de prefixos gerenciados.
3. Marque a caixa de seleção da lista de prefixos e escolha Actions (Ações), Restore prefix list (Restaurar lista de prefixos).
4. Em Select prefix list version (Selecionar versão da lista de prefixos), escolha uma versão anterior. As entradas para a versão selecionada são exibidas em Prefix list entries (Entradas da lista de prefixos).
5. Escolha Restaurar lista de prefixos.

Como restaurar uma versão anterior de lista de prefixos usando a AWS CLI

Use o comando restore-managed-prefix-list-version.

Excluir uma lista de prefixos

Para excluir uma lista de prefixos, você deve primeiro remover quaisquer referências a ela nos recursos (por exemplo, nas tabelas de rotas). Caso você tenha compartilhado a lista de prefixos usando o AWS RAM, todas as referências em recursos que pertençam ao consumidor devem ser removidas primeiro.

Limitação

Não é possível excluir uma lista de prefixos gerenciados pela AWS.

Como excluir uma lista de prefixos usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Listas de prefixos gerenciados.

3. Selecione a lista de prefixos e escolha Ações, Excluir lista de prefixos.
4. Na caixa de diálogo de confirmação, insira `delete` e selecione Excluir.

Como excluir uma lista de prefixos usando a AWS CLI

Use o comando delete-managed-prefix-list.

Compartilhar listas de prefixos gerenciadas pelo cliente

Com o AWS Resource Access Manager (AWS RAM), o proprietário de uma lista de prefixos gerenciada pelo cliente pode compartilhar uma lista de prefixos com o seguinte:

- Contas específicas da AWS dentro ou fora de sua organização no AWS Organizations
- Uma unidade organizacional dentro da organização no AWS Organizations
- Uma organização inteira no AWS Organizations

Os consumidores com quem uma lista de prefixos foi compartilhada podem visualizar a lista de prefixos e suas entradas e podem fazer referência à lista de prefixos em seus recursos da AWS.

Para obter mais informações sobre o AWS RAM, consulte o Guia do usuário do AWS RAM. Para obter mais informações, consulte Service Quotas no Guia do usuário do AWS RAM.

> **Important**
>
> Não há cobranças adicionais pelo compartilhamento de listas de prefixos.

Conteúdo

Permissões de lista de prefixos compartilhada

Permissões para proprietários

Os proprietários são responsáveis por gerenciar uma lista de prefixos compartilhada e suas entradas. Os proprietários podem visualizar os IDs dos recursos da AWS que fazem referência à lista de

prefixos. No entanto, eles não podem adicionar ou remover referências a uma lista de prefixos de propriedade dos consumidores nos recursos da AWS.

Os proprietários não podem excluir uma lista de prefixos se a lista de prefixos é referenciada em um recurso que pertence a um consumidor.

Permissões para consumidores

Os consumidores podem visualizar as entradas em uma lista de prefixos compartilhada e podem fazer referência a uma lista de prefixos compartilhada nos recursos da AWS. No entanto, eles não podem modificar, restaurar ou excluir uma lista de prefixos compartilhada.

Trabalhar com listas de prefixos compartilhadas

As listas de prefixos da AWS fornecem uma maneira conveniente de gerenciar e referenciar os intervalos de endereços IP usados por vários serviços da AWS. Além das listas de prefixos gerenciados pela AWS, você também pode criar e compartilhar suas próprias listas de prefixos gerenciadas pelo cliente com outras contas da AWS.

O compartilhamento de listas de prefixos pode ser particularmente útil para organizações com requisitos complexos de rede ou aquelas que precisam coordenar o uso de endereços IP em várias workloads da AWS. Ao compartilhar uma lista de prefixos, você pode garantir um gerenciamento consistente de endereços IP e simplificar as configurações de rede para seus colaboradores.

Esta seção descreve como compartilhar listas de prefixos e como identificar e usar listas de prefixos que foram compartilhadas com sua conta.

Conteúdo

Compartilhar uma lista de prefixos

Para compartilhar uma lista de prefixos, é necessário adicioná-la a um compartilhamento de recursos. Caso você não tenha um compartilhamento de recursos, primeiro será necessário criar um usando o console do AWS RAM.

Se você fizer parte de uma organização no AWS Organizations e o compartilhamento estiver habilitado na organização, os consumidores da organização receberão acesso automaticamente à lista de prefixos compartilhada. Caso contrário, os consumidores receberão um convite para participar do compartilhamento de recursos e acesso à lista de prefixos compartilhada depois de aceitar o convite.

Você pode criar um compartilhamento de recursos e compartilhar uma lista de prefixos de sua propriedade usando o console do AWS RAM ou a AWS CLI.

Important

- Para compartilhar uma lista de prefixos, é necessário ser o proprietário dela. Não é possível compartilhar uma lista de prefixos que tenha sido compartilhada com você. Não é possível compartilhar uma lista de prefixos gerenciados pela AWS.
- Para compartilhar uma lista de prefixos com a sua organização ou com uma unidade organizacional no AWS Organizations, é necessário habilitar o compartilhamento com o AWS Organizations. Para obter mais informações, consulte Habilitar o compartilhamento com o AWS Organizations no Manual do usuário do AWS RAM.

Como criar um compartilhamento de recursos e compartilhar uma lista de prefixos usando o console do AWS RAM

Siga as etapas em Criar um compartilhamento de recursos no Manual do usuário do AWS RAM. Em Selecionar tipo de recurso, escolha Listas de prefixos e marque a caixa de seleção da sua lista de prefixos.

Como adicionar uma lista de prefixos a um compartilhamento de recursos existente usando o console do AWS RAM

Para adicionar um prefixo gerenciado pertencente a você a um compartilhamento de recursos existente, siga as etapas em Atualização de um compartilhamento de recursos no Manual do usuário do AWS RAM. Em Selecionar tipo de recurso, escolha Listas de prefixos e marque a caixa de seleção da sua lista de prefixos.

Como compartilhar uma lista de prefixos de sua propriedade usando a AWS CLI

Use os comandos a seguir para criar e atualizar um compartilhamento de recursos:

- create-resource-share
- associate-resource-share
- update-resource-share

Cancelar o compartilhamento de uma lista de prefixos compartilhada

Quando você cancela o compartilhamento de uma lista de prefixos, os consumidores não podem mais visualizar a lista de prefixos ou suas entradas na conta, além disso, eles não podem fazer referência à lista de prefixos nos recursos. Se a lista de prefixos já estiver referenciada nos recursos do consumidor, essas referências continuarão a funcionar normalmente e você poderá continuar a visualizar essas referências. Se você atualizar a lista de prefixos para uma nova versão, as referências usarão a versão mais recente.

Para cancelar o compartilhamento de uma lista de prefixos pertencente a você, é necessário removê-la do compartilhamento de recursos usando o AWS RAM.

Como cancelar o compartilhamento de uma lista de prefixos de sua propriedade usando o console do AWS RAM

Consulte Atualização de um compartilhamento de recursos no Manual do usuário do AWS RAM.

Como cancelar o compartilhamento de uma lista de prefixos de sua propriedade usando a AWS CLI

Use o comando disassociate-resource-share.

Identificar uma lista de prefixos compartilhada

Os proprietários e os consumidores podem identificar listas de prefixos compartilhadas usando o console da Amazon VPC e a AWS CLI.

Como identificar uma lista de prefixos compartilhada usando o console da Amazon VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Listas de prefixos gerenciados.
3. A página exibe as listas de prefixos que você possui e as listas de prefixos compartilhadas com você. A coluna ID do proprietário mostra o ID de conta da AWS do proprietário da lista de prefixos.
4. Para visualizar as informações de compartilhamento de recursos de uma lista de prefixos, selecione a lista de prefixos e escolha Compartilhamento no painel inferior.

Como identificar uma lista de prefixos compartilhada usando a AWS CLI

Use o comando describe-managed-prefix-lists. O comando retorna as listas de prefixos que você possui e as listas de prefixos compartilhadas com você. O `OwnerId` mostra o ID da conta da AWS do proprietário da lista de prefixos.

Identificar referências a uma lista de prefixos compartilhada

Os proprietários podem identificar os recursos que pertencem ao consumidor que fazem referência a uma lista de prefixos compartilhada.

Como identificar referências a uma lista de prefixos compartilhada usando o console da Amazon VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Listas de prefixos gerenciados.
3. Selecione a lista de prefixos e escolha Associações no painel inferior.
4. Os IDs dos recursos que fazem referência à lista de prefixos estão listados na coluna ID de recurso . Os proprietários dos recursos estão listados na coluna Proprietário do recurso.

Como identificar referências a uma lista de prefixos compartilhada usando a AWS CLI

Use o comando get-managed-prefix-list-associations.

Listas de prefixos gerenciados pela AWS

Listas de prefixos gerenciados pela AWS são conjuntos de intervalos de endereços IP para produtos da AWS. Essas listas de prefixos são mantidas pela Amazon Web Services e fornecem uma forma de referenciar os endereços IP usados por várias ofertas da AWS. Isso pode ser particularmente útil ao configurar grupos de segurança ou outros controles no nível da rede em uma VPC.

As listas de prefixos abrangem uma ampla variedade de serviços da AWS, incluindo S3, DynamoDB e muitos outros. Ao usar as listas de prefixos gerenciadas, é possível garantir que suas configurações de rede estejam atualizadas e contabilizem adequadamente os endereços IP usados pelos serviços da AWS dos quais você depende. Isso pode ajudar a simplificar as tarefas de rede e reduzir a sobrecarga administrativa da manutenção manual de listas de endereços IP.

Além dos benefícios práticos, o uso de listas de prefixos gerenciados também se alinha às práticas recomendadas de segurança da AWS. Ao confiar nas informações oficiais de endereço IP fornecidas

pela AWS, é possível minimizar o risco de configurações incorretas ou problemas inesperados de conectividade. Isso pode ser especialmente importante para aplicações de missão crítica ou workloads com requisitos rígidos de conformidade.

Conteúdo

Listas de prefixos gerenciados pela AWS disponíveis

Os seguintes serviços fornecem listas de prefixos gerenciados pela AWS.

AWS service (Serviço da AWS)	Nome da lista de prefixos	Weight
Amazon CloudFront	com.amazonaws.global.cloudfront.origin-facing	55
Amazon DynamoDB	com.amazonaws.*region*.dynamodb	1
Amazon EC2 Instance Connect	com.amazonaws.*region*.ec2-instance-connect	2
	com.amazonaws.*region*.ipv6.ec2-instance-connect	2
AWS Ground Station	com.amazonaws.global.groundstation	5
Amazon Route 53	com.amazonaws.*region*.ipv6.route53-healthchecks	25
	com.amazonaws.*region*.route53-healthchecks	25
Amazon S3	com.amazonaws.*region*.s3	1
Amazon S3 Express One Zone	com.amazonaws.*region*.s3express	6
Amazon VPC Lattice	com.amazonaws.*região*.vpc-lattice	10
	com.amazonaws.*region*.ipv6.vpc-lattice	10

Para visualizar listas de prefixos gerenciadas pela AWS usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Listas de prefixos gerenciados.
3. No campo de pesquisa, adicione o filtro Owner ID: AWS (ID do proprietário).

Para visualizar listas de prefixos gerenciadas pela AWS usando a AWS CLI

Use o comando describe-managed-prefix-lists como descrito a seguir.

```
aws ec2 describe-managed-prefix-lists --filters Name=owner-id,Values=AWS
```

Peso da lista de prefixos gerenciados pela AWS

O peso da lista de prefixos gerenciados pela AWS se refere ao número de entradas que ela ocupa em um recurso.

Por exemplo, o peso de uma lista de prefixos gerenciados pelo Amazon CloudFront é 55. Veja como isso afeta suas cotas da Amazon VPC:

- Grupos de segurança: a cota padrão é de 60 regras, deixando espaço para apenas cinco regras adicionais em um grupo de segurança. Você pode solicitar um aumento dessa cota.
- Tabelas de rotas: a cota padrão é de 50 rotas, então você deve solicitar um aumento de cota para que possa adicionar a lista de prefixos a uma tabela de rotas.

Usar uma lista de prefixos gerenciados pela AWS

As listas de prefixos gerenciados pela AWS são criadas e mantidas pela AWS e podem ser usadas por qualquer pessoa com uma conta da AWS. Não é possível criar, modificar, compartilhar ou excluir uma lista de prefixos gerenciados pela AWS.

Assim como acontece com as listas de prefixos gerenciados pelo cliente, as listas de prefixos gerenciados pela AWS podem ser usadas com recursos da AWS, como grupos de segurança e tabelas de rotas. Para ter mais informações, consulte Otimizar o gerenciamento da infraestrutura da AWS com listas de prefixos.

Otimizar o gerenciamento da infraestrutura da AWS com listas de prefixos

É possível fazer referência a uma lista de prefixos nos recursos da AWS a seguir.

Recursos

- Grupos de segurança da VPC
- Tabelas de rotas de sub-rede
- Tabela de rotas do gateway de trânsito
- Grupos de regras do AWS Network Firewall
- Controle de acesso à rede para o Amazon Managed Grafana
- Gateways locais do rack AWS Outposts

Grupos de segurança da VPC

É possível especificar uma lista de prefixos como origem de uma regra de entrada ou como destino de uma regra de saída. Para ter mais informações, consulte Grupos de segurança.

> **Important**
>
> Não é possível modificar uma regra existente para usar uma lista de prefixos. É necessário criar uma nova regra para usar uma lista de prefixos.

Como fazer referência a uma lista de prefixos em uma regra de grupo de segurança usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione o security group para atualizar.
4. Selecione Actions (Ações), Edit inbound rules (Editar regras de entrada) ou Actions (Ações), Edit outbound rules (Editar regras de saída).
5. Escolha Add rule (Adicionar regra). Em Tipo, selecione o tipo de tráfego. Em Origem (regras de entrada) ou Destino (regras de saída), escolha Personalizado. Em seguida, no próximo campo, em Listas de prefixos, selecione o ID da lista de prefixos.
6. Escolha Save rules (Salvar regras).

Como fazer referência a uma lista de prefixos em uma regra de grupo de segurança usando a AWS CLI

Use os comandos authorize-security-group-ingress e authorize-security-group-egress. Para o parâmetro `--ip-permissions`, especifique o ID da lista de prefixos usando `PrefixListIds`.

Tabelas de rotas de sub-rede

É possível especificar uma lista de prefixos como destino para a entrada da tabela de rotas. Não é possível fazer referência a uma lista de prefixos em uma tabela de rotas do gateway. Para obter mais informações sobre tabelas de rotas, consulte Configurar tabelas de rotas.

Como fazer referência a uma lista de prefixos em uma tabela de rotas usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Route Tables (Tabelas de rotas) e selecione a tabela de rotas.
3. Selecione Actions (Ações), Edit routes (Editar rotas).
4. Para adicionar uma rota, escolha Add route (Adicionar rota).
5. Em Destino, insira o ID de uma lista de prefixos.
6. Em Target (alvo), escolha um alvo.
7. Escolha Salvar alterações.

Como fazer referência a uma lista de prefixos em uma tabela de rotas usando a AWS CLI

Use o comando create-route (AWS CLI). Use o parâmetro `--destination-prefix-list-id` para especificar o ID de uma lista de prefixos.

Tabela de rotas do gateway de trânsito

É possível especificar uma lista de prefixos como o destino de uma rota. Para obter mais informações, consulte Referências de lista de prefixos em Gateways de trânsito da Amazon VPC.

Grupos de regras do AWS Network Firewall

Um grupo de regras AWS Network Firewall é um conjunto reutilizável de critérios para inspecionar e lidar com o tráfego de rede. Se você criar grupos de regras com estado compatíveis com Suricata no AWS Network Firewall, é possível fazer referência a uma lista de prefixos do grupo de regras. Para obter mais informações, consulte Referenciar listas de prefixo da Amazon VPC e Criar um grupo de regras com estado no Guia do desenvolvedor do AWS Network Firewall.

Controle de acesso à rede para o Amazon Managed Grafana

Você pode especificar uma ou mais listas de prefixos como uma regra de entrada para solicitações aos espaços de trabalho do Amazon Managed Grafana. Para obter mais informações sobre o controle de acesso à rede do espaço de trabalho do Grafana, incluindo como referenciar listas de prefixos, consulte Gerenciamento do acesso à rede no Guia do usuário do Amazon Managed Grafana.

Gateways locais do rack AWS Outposts

Cada rack AWS Outposts fornece um gateway local que permite conectar seus recursos do Outpost às suas redes on-premises. Você pode agrupar os CIDRs que usa com frequência em uma lista de prefixos e referenciar essa lista como um destino de rota na tabela de rotas do gateway local. Para obter mais informações, consulte Gerenciar rotas da tabela de rotas do gateway local no Guia do usuário dos racks do AWS Outposts.

Intervalos de endereços IP da AWS

A AWS publica seus intervalos de endereços IP atuais em formato JSON. Com essas informações, é possível identificar o tráfego da AWS. Você também pode usar essas informações para permitir ou negar tráfego de entrada ou de saída de alguns serviços da Serviços da AWS.

Considerações

- Publicamos os intervalos de endereços IP dos serviços que os clientes normalmente usam para realizar a filtragem de saída. Não publicamos os intervalos de endereços IP para todos os serviços.
- Os serviços podem usar os intervalos de endereços IP para se comunicar com outros serviços ou com a rede de um cliente.
- Os intervalos de endereços IP que você traz para a AWS por meio de “traga seus próprios endereços IP” (BYOIP) não estão incluídos no arquivo `.json`. Para obter mais informações, consulte Anunciar o intervalo de endereços por meio da AWS no Guia do usuário do Amazon EC2.

Alguns serviços publicam seus intervalos de endereços usando listas de prefixos gerenciadas pela AWS. Para ter mais informações, consulte the section called “Listas de prefixos gerenciados pela AWS disponíveis”.

Conteúdo

Baixe o arquivo JSON

Para visualizar os intervalos de endereços atuais, baixe ip-ranges.json. Para manter o histórico, salve as sucessivas versões do arquivo .JSON no seu sistema. Para determinar se eles foram alterados desde a última vez que você salvou o arquivo, marque a hora da publicação no arquivo atual e compare-a com a hora da publicação no último arquivo que você salvou.

O exemplo de comando curl a seguir salva o arquivo JSON no diretório atual.

```
curl -O https://ip-ranges.amazonaws.com/ip-ranges.json
```

Se você acessar esse arquivo programaticamente, é sua responsabilidade garantir que o aplicativo faz download do arquivo somente após a verificação bem-sucedida do certificado TLS apresentado pelo servidor.

Para receber notificações de atualizações no arquivo JSON, consulte the section called “Assinar notificações do ”.

Controle de saída

Para permitir que os recursos que você criou com um serviço da AWS só acessem outros serviços da AWS, você pode usar as informações do intervalo de endereços IP no arquivo ip-ranges.json para realizar a filtragem de saída. Certifique-se de que as regras do grupo de segurança permitam tráfego de saída para os blocos CIDR na lista AMAZON. Existem cotas para grupos de segurança. Dependendo do número de intervalos de endereços IP em cada região, talvez vários grupos de segurança sejam necessários por região.

> **Note**
>
> Alguns serviços da AWS são criados no EC2 e usam o espaço de endereço IP do EC2. Se você bloquear o tráfego para o espaço de endereço IP do EC2, também bloqueará o tráfego para esses serviços que não são do EC2.

Feed de geolocalização

Os intervalos de endereços IP em `ip-ranges.json` são por Região da AWS. No entanto, uma zona local não está no mesmo local físico de sua região principal. Os dados de geolocalização publicados em geo-ip-feed.csv representam as zonas Locais. Os dados seguem a RFC 8805.

Descobrir os intervalos de endereços IP para os Serviços da AWS

O arquivo JSON de intervalos de endereços IP da AWS fornecido pela AWS pode ser um recurso valioso para descobrir os endereços IP de vários serviços da AWS e utilizar essas informações para aprimorar a segurança e o controle de acesso da sua rede. Analisando os dados detalhados contidos nesse arquivo JSON, você pode identificar com precisão os intervalos de endereços IP associados a serviços e regiões específicas da Serviços da AWS.

Por exemplo, você pode utilizar os intervalos de endereços IP para configurar políticas robustas de segurança de rede, configurando regras granulares de firewall para permitir ou negar acesso a determinados recursos da AWS. Essas informações também podem ser úteis para toda uma variedade de tarefas da AWS Network Firewall. Esse nível de controle é essencial para proteger dados e aplicações, garantindo que somente tráfego autorizado possa alcançar os serviços da Serviços da AWS necessários. Além disso, ter essa inteligência de IP pode ajudar a garantir que suas aplicações sejam configuradas adequadamente para se comunicar com os endpoints da AWS certos, melhorando a confiabilidade e a performance gerais.

Além das regras de firewall, o arquivo `ip-ranges.json` também pode ser usado para configurar uma filtragem de saída sofisticada na infraestrutura de rede. Entendendo os intervalos de endereços IP de destino para os diferentes Serviços da AWS, você poderá configurar políticas de roteamento ou utilizar soluções avançadas de segurança de rede, como permitir ou bloquear seletivamente o tráfego de saída com base no destino pretendido. Esse controle de saída é essencial para reduzir o risco de vazamento de dados e acesso não autorizado.

É importante observar que o arquivo `ip-ranges.json` é atualizado regularmente, assim sendo, manter uma cópia local atualizada é essencial para garantir que você tenha as informações mais

precisas e atuais. Ao aproveitar continuamente o conteúdo desse arquivo, você pode gerenciar com eficiência o acesso à rede e a segurança das suas aplicações baseadas na AWS, fortalecendo sua postura geral de segurança na nuvem.

Os exemplos a seguir podem ajudar você a filtrar os intervalos de endereços IP da AWS para obter apenas o que você está procurando. No Linux, você pode baixar e usar a ferramenta jq para analisar uma cópia local do arquivo JSON. O AWS Tools for Windows PowerShell inclui um cmdlet, Get-AWSPublicIpAddressRange, que você pode usar para analisar esse arquivo JSON. Para obter mais informações, consulte Querying the Public IP Address Ranges for AWS.

Para obter o arquivo JSON, consulte the section called “Baixar”. Para obter mais informações sobre a sintaxe do arquivo JSON, consulte the section called “Sintaxe”.

Exemplos

- Obter a data de criação do arquivo
- Obter os endereços IP de uma região específica
- Obter todos os endereços IPv4
- Obter todos os endereços IPv4 de um serviço específico
- Obter todos os endereços IPv4 de um serviço específico em uma Região específica
- Obter todos os endereços IPv6
- Obter todos os endereços IPv6 de um serviço específico
- Obter todos os endereços IP de um grupo fronteiriço específico

Obter a data de criação do arquivo

O exemplo a seguir obtém a data de criação do arquivo `ip-ranges.json`.

jq

```
$ jq .createDate < ip-ranges.json

"2024-08-01-17-22-15"
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -OutputPublicationDate
```

```
Thursday, August 1, 2024 9:22:35 PM
```

Obter os endereços IP de uma região específica

O exemplo a seguir filtra o arquivo JSON para obter os endereços IP da região especificada.

jq

```
$ jq '.prefixes[] | select(.region=="us-east-1")' < ip-ranges.json

{
  "ip_prefix": "23.20.0.0/14",
  "region": "us-east-1",
  "network_border_group": "us-east-1",
  "service": "AMAZON"
},
{
  "ip_prefix": "50.16.0.0/15",
  "region": "us-east-1",
  "network_border_group": "us-east-1",
  "service": "AMAZON"
},
{
  "ip_prefix": "50.19.0.0/16",
  "region": "us-east-1",
  "network_border_group": "us-east-1",
  "service": "AMAZON"
},
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -Region us-east-1

IpPrefix        Region      NetworkBorderGroup         Service
--------        ------       -------                   -------
23.20.0.0/14    us-east-1    us-east-1                 AMAZON
50.16.0.0/15    us-east-1    us-east-1                 AMAZON
50.19.0.0/16    us-east-1    us-east-1                 AMAZON
...
```

Obter todos os endereços IPv4

O exemplo a seguir filtra o arquivo JSON para obter os endereços IPv4.

jq

```
$ jq -r '.prefixes | .[].ip_prefix' < ip-ranges.json

23.20.0.0/14
27.0.0.0/22
43.250.192.0/24
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange | where {$_.IpAddressFormat -eq "Ipv4"} | select
 IpPrefix

IpPrefix
--------
23.20.0.0/14
27.0.0.0/22
43.250.192.0/24
...
```

Obter todos os endereços IPv4 de um serviço específico

O exemplo a seguir filtra o arquivo JSON para obter os endereços IPv4 do serviço especificado.

jq

```
$ jq -r '.prefixes[] | select(.service=="GLOBALACCELERATOR") | .ip_prefix' < ip-
ranges.json

13.248.117.0/24
15.197.34.0/23
15.197.36.0/22
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -ServiceKey GLOBALACCELERATOR | where
 {$_.IpAddressFormat -eq "Ipv4"} | select IpPrefix

IpPrefix
--------
13.248.117.0/24
15.197.34.0/23
15.197.36.0/22
...
```

Obter todos os endereços IPv4 de um serviço específico em uma Região específica

O exemplo a seguir filtra o arquivo JSON para obter os endereços IPv4 do serviço especificado na região especificada.

jq

```
$ jq -r '.prefixes[] | select(.region=="us-east-1") |
 select(.service=="GLOBALACCELERATOR") | .ip_prefix' < ip-ranges.json

13.248.124.0/24
99.82.166.0/24
99.82.171.0/24
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -Region us-east-1 -ServiceKey GLOBALACCELERATOR
 | where {$_.IpAddressFormat -eq "Ipv4"} | select IpPrefix

IpPrefix
--------
13.248.117.0/24
99.82.166.0/24
99.82.171.0/24
...
```

Obter todos os endereços IPv6

O exemplo a seguir filtra o arquivo JSON para obter os endereços IPv6.

jq

```
$ jq -r '.ipv6_prefixes | .[].ipv6_prefix' < ip-ranges.json

2a05:d07c:2000::/40
2a05:d000:8000::/40
2406:dafe:2000::/40
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange | where {$_.IpAddressFormat -eq "Ipv6"} | select
 IpPrefix

IpPrefix
--------
2a05:d07c:2000::/40
2a05:d000:8000::/40
2406:dafe:2000::/40
...
```

Obter todos os endereços IPv6 de um serviço específico

O exemplo a seguir filtra o arquivo JSON para obter os endereços IPv6 do serviço especificado.

jq

```
$ jq -r '.ipv6_prefixes[] | select(.service=="GLOBALACCELERATOR") | .ipv6_prefix' <
 ip-ranges.json

2600:1f01:4874::/47
2600:1f01:4802::/47
2600:1f01:4860::/47
2600:9000:a800::/40
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -ServiceKey GLOBALACCELERATOR | where
 {$_.IpAddressFormat -eq "Ipv6"} | select IpPrefix

IpPrefix
--------
2600:1f01:4874::/47
2600:1f01:4802::/47
2600:1f01:4860::/47
2600:9000:a800::/40
...
```

Obter todos os endereços IP de um grupo fronteiriço específico

O exemplo a seguir filtra o arquivo JSON para obter todos os endereços IP do grupo fronteiriço especificado.

jq

```
$ jq -r '.prefixes[] | select(.network_border_group=="us-west-2-lax-1")
 | .ip_prefix' < ip-ranges.json
70.224.192.0/18
52.95.230.0/24
15.253.0.0/16
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange | where {$_.NetworkBorderGroup -eq "us-west-2-
lax-1"} | select IpPrefix

IpPrefix
--------
70.224.192.0/18
52.95.230.0/24
15.253.0.0/16
...
```

Sintaxe para o intervalo de endereços IP da AWS em JSON

A AWS publica seus intervalos de endereços IP atuais em formato JSON. Para obter o arquivo JSON, consulte the section called “Baixar”. Segue abaixo a sintaxe do arquivo JSON.

```
{
  "syncToken": "0123456789",
  "createDate": "yyyy-mm-dd-hh-mm-ss",
  "prefixes": [
    {
      "ip_prefix": "cidr",
      "region": "region",
      "network_border_group": "network_border_group",
      "service": "subset"
    }
  ],
  "ipv6_prefixes": [
    {
      "ipv6_prefix": "cidr",
      "region": "region",
      "network_border_group": "network_border_group",
      "service": "subset"
    }
  ]
}
```

syncToken

A hora da publicação em formato de horário epoch Unix.

Tipo: string

Example: `"syncToken": "1416435608"`

createDate

A data e hora da publicação, no formato UTC AA-MM-DD-hh-mm-ss.

Tipo: string

Example: `"createDate": "2014-11-19-23-29-02"`

prefixos

Os prefixos IP para os intervalos de endereços IPv4.

Tipo: matriz

ipv6_prefixes

Os prefixos IP para os intervalos de endereços IPv6.

Tipo: matriz

ip_prefix

O intervalo de endereços IPv4 públicos, na notação CIDR. Observe que a AWS pode publicar um prefixo em intervalos mais específicos. Por exemplo, o prefixo 96.127.0.0/17 no arquivo pode ser publicado como 96.127.0.0/21, 96.127.8.0/21, 96.127.32.0/19 e 96.127.64.0/18.

Tipo: string

Example: `"ip_prefix": "198.51.100.2/24"`

ipv6_prefix

O intervalo de endereços IPv6 públicos, na notação CIDR. Observe que a AWS pode publicar um prefixo em intervalos mais específicos.

Tipo: string

Example: `"ipv6_prefix": "2001:db8:1234::/64"`

network_border_group

O nome do grupo de borda de rede, que é um conjunto exclusivo de zonas de disponibilidade ou zonas locais das quais a AWS publica endereços IP ou `GLOBAL`. O tráfego para serviços `GLOBAL` pode ser originado ou atraído para várias (até todas) zonas de disponibilidade ou zonas locais das quais a AWS publica endereços IP.

Tipo: string

Example: `"network_border_group": "us-west-2-lax-1"`

região

A região da AWS ou `GLOBAL`. O tráfego para serviços `GLOBAL` pode ser originado ou atraído para várias (até todas) as regiões da AWS.

Tipo: string

Valores válidos: `af-south-1` | `ap-east-1` | `ap-northeast-1` | `ap-northeast-2` | `ap-northeast-3` | `ap-south-1` | `ap-south-2` | `ap-southeast-1` | `ap-southeast-2` | `ap-`

southeast-3 | ap-southeast-4 | ap-southeast-5 | ap-southeast-7 ca-central-1 | ca-west-1 | cn-north-1 | cn-northwest-1 | eu-central-1 | eu-central-2 | eu-north-1 | eu-south-1 | eu-south-2 | eu-west-1 | eu-west-2 | eu-west-3 | il-central-1 | mx-central-1 | me-central-1 | me-south-1 | sa-east-1 | us-east-1 | us-east-2 | us-gov-east-1 | us-gov-west-1 | us-west-1 | us-west-2 | GLOBAL

Example: `"region": "us-east-1"`

serviço

O subconjunto de intervalos de endereços IP. Os endereços listados para a API_GATEWAY são apenas de saída. Especifique AMAZON para obter todos os intervalos de endereços IP (o que significa que cada subconjunto também está no subconjunto AMAZON). No entanto, alguns intervalos de endereços IP estão apenas no subconjunto AMAZON (o que significa que eles também não estão disponíveis em outro subconjunto).

Tipo: string

Valores válidos: AMAZON | AMAZON_APPFLOW | AMAZON_CONNECT | API_GATEWAY | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CLOUDFRONT_ORIGIN_FACING | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR | IVS_REALTIME | KINESIS_VIDEO_STREAMS | MEDIA_PACKAGE_V2 | ROUTE53 | ROUTE53_HEALTHCHECKS | ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_RESOLVER | S3 | WORKSPACES_GATEWAYS

Example: `"service": "AMAZON"`

Sobreposições de intervalos

Os intervalos de endereços IP retornados por qualquer código de serviço também são retornados pelo código de serviço AMAZON. Por exemplo, todos os intervalos de endereços IP retornados pelo código de serviço S3 também são retornados pelo código de serviço AMAZON.

Quando o serviço A usa recursos do serviço B, há intervalos de endereços IP que são retornados pelos códigos de serviço para o serviço A e o serviço B. Porém, esses intervalos de endereços IP são usados exclusivamente pelo serviço A e não podem ser usados pelo serviço B. Por exemplo, o Amazon S3 usa recursos do Amazon EC2 e, portanto, há intervalos de endereços IP que são retornados pelo códigos de serviço S3 e EC2. Porém, esses intervalos de endereços IP são usados exclusivamente pelo Amazon S3. Portanto, o código de serviço S3 retorna todos os intervalos de

endereços IP usados exclusivamente pelo Amazon S3. Para identificar os intervalos de endereços IP que são usados exclusivamente pelo Amazon EC2, localize aqueles que são retornados pelo código de serviço `EC2`, mas não pelo código de serviço `S3`.

Saiba mais

Esta seção fornece links para informações adicionais sobre diferentes códigos de serviço.

- `AMAZON_APPFLOW`: Intervalos de endereços IP
- `AMAZON_CONNECT`: Configurar sua rede
- `CHIME_MEETINGS` — Configuração para mídia e sinalização
- `CLOUDFRONT`: Localizações e intervalos de endereço IP dos servidores de borda do CloudFront
- `DYNAMODB`: Intervalos de endereços IP
- `EC2`: Endereços IPv4 públicos
- `EC2_INSTANCE_CONNECT` — Pré-requisitos do EC2 Instance Connect
- `GLOBALACCELERATOR`: Localizações e intervalos de endereços IP dos servidores de borda do Global Accelerator
- `ROUTE53`: Intervalos de endereço IP dos servidores do Amazon Route 53
- `ROUTE53_HEALTHCHECKS`: Intervalos de endereço IP dos servidores do Amazon Route 53
- `ROUTE53_HEALTHCHECKS_PUBLISHING`: Intervalos de endereço IP dos servidores do Amazon Route 53
- `WORKSPACES_GATEWAYS`: Servidores de gateway PCoIP

Notas da versão

A tabela a seguir descreve as atualizações da sintaxe do `ip-ranges.json`. Também adicionamos novos códigos de região com cada lançamento da região.

Descrição	Data de lançamento
Adicionado o código de serviço `IVS_REALTIME` .	11 de junho de 2024
Adicionado o código de serviço `MEDIA_PACKAGE_V2` .	9 de maio de 2023

Descrição	Data de lançamento
Adicionado o código de serviço `CLOUDFRONT_ORIGIN_FACING` .	12 de outubro de 2021
Adicionado o código de serviço `ROUTE53_RESOLVER` .	24 de junho de 2021
Adicionado o código de serviço `EBS`.	12 de maio de 2021
Adicionado o código de serviço `KINESIS_VIDEO_STREAMS` .	19 de novembro de 2020
Adicionados os códigos de serviço `CHIME_MEETINGS` e `CHIME_VOICECONNECTOR` .	19 de junho de 2020
Adicionado o código de serviço `AMAZON_APPFLOW` .	9 de junho de 2020
Adicione suporte para o grupo de borda de rede.	7 de abril de 2020
Adicionado o código de serviço `WORKSPACES_GATEWAYS` .	30 de março de 2020
Adicionado o código de serviço `ROUTE53_HEALTHCHECK_PUBLISHING` .	30 de janeiro de 2020
Adicionado o código de serviço `API_GATEWAY` .	26 de setembro de 2019
Adicionado o código de serviço `EC2_INSTANCE_CONNECT` .	26 de junho de 2019
Adicionado o código de serviço `DYNAMODB`.	25 de abril de 2019
Adicionado o código de serviço `GLOBALACCELERATOR` .	20 de dezembro de 2018

Descrição	Data de lançamento
Adicionado o código de serviço AMAZON_CONNECT .	20 de junho de 2018
Adicionado o código de serviço CLOUD9.	20 de junho de 2018
Adicionado o código de serviço CODEBUILD .	19 de abril de 2018
Adicionado o código de serviço S3.	28 de fevereiro de 2017
Adicionado suporte para intervalos de endereços IPv6.	22 de agosto de 2016
Lançamento inicial	19 de novembro de 2014

Notificações de intervalos de endereços IP da AWS

A AWS publica seus intervalos de endereços IP atuais em formato JSON. Sempre que houver uma alteração em intervalos de endereços IP da AWS, poderemos enviar notificações para os assinantes do tópico do Amazon SNS intitulado AmazonIpSpaceChanged. Para obter mais informações sobre a sintaxe do arquivo JSON, consulte the section called “Sintaxe”.

A carga útil da notificação contém informações no formato a seguir.

```
{
  "create-time":"yyyy-mm-ddThh:mm:ss+00:00",
  "synctoken":"0123456789",
  "md5":"6a45316e8bc9463c9e926d5d37836d33",
  "url":"https://ip-ranges.amazonaws.com/ip-ranges.json"
}
```

create-time

A data e hora de criação.

As notificações podem ser entregues fora de ordem. Portanto, recomendamos que você verifique as marcas de data/hora para garantir a ordem correta.

synctoken

A hora da publicação em formato de horário epoch Unix.

md5

O valor de hash criptográfico do arquivo `ip-ranges.json`. Você pode usar esse valor para verificar se o arquivo baixado está corrompido.

url

A localização do arquivo `ip-ranges.json`. Para ter mais informações, consulte the section called “Baixar”.

Você pode se inscrever para receber notificações da seguinte forma.

Para assinar as notificações de intervalo de endereço IP da AWS

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. É necessário selecionar esta Região porque as notificações do SNS que você está assinando foram criadas nesta Região.
3. No painel de navegação, escolha Subscriptions.
4. Selecione Create subscription.
5. Na caixa de diálogo Criar assinatura, faça o seguinte:
   a. Para o ARN do tópico, copie o seguinte ARN (nome de recurso da Amazon):

      ```
      arn:aws:sns:us-east-1:806199016981:AmazonIpSpaceChanged
      ```

   b. Para o Protocolo, escolha o protocolo a ser usado (por exemplo, `Email`).
   c. Para o Endpoint, digite o endpoint no qual receber a notificação (por exemplo, seu endereço de e-mail).
   d. Selecione Criar assinatura.
6. Você será contatado no endpoint especificado, pedindo que confirme sua assinatura. Por exemplo, se você tiver especificado um endereço de e-mail, receberá uma mensagem de e-mail com a linha de assunto `AWS Notification - Subscription Confirmation`. Siga as instruções para confirmar sua assinatura.

As notificações estão sujeitas à disponibilidade do endpoint. Portanto, você deve verificar o arquivo JSON periodicamente para garantir que tem os intervalos mais recentes. Para obter mais informações sobre confiabilidade do Amazon SNS, consulte https://aws.amazon.com/sns/faqs/#Reliability.

Se não deseja mais receber essas notificações, use o procedimento a seguir para cancelar a assinatura.

Para cancelar a assinatura de notificações de intervalos de endereço IP da AWS

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. No painel de navegação, escolha Assinaturas.
3. Marque a caixa de seleção da assinatura.
4. Selecione Ações, Excluir assinaturas.
5. Quando a confirmação for solicitada, escolha Excluir.

Para obter mais informações sobre tópicos do Amazon SNS, consulte o Guia do desenvolvedor do Amazon Simple Notification Service.

Suporte a IPv6 para sua VPC

Se você possuir uma VPC que ofereça suporte somente a IPv4 e recursos na sub-rede que sejam configurados para usar somente o IPv4, poderá adicionar o suporte a IPv6 para a VPC e seus recursos. A VPC pode operar em modo de pilha dual: os seus recursos podem se comunicar por IPv4, IPv6 ou ambos. A comunicação IPv4 é independente da comunicação IPv6.

Não é possível desabilitar o suporte IPv4 para a VPC e as sub-redes. Este é o sistema de endereçamento IP padrão para a Amazon VPC e o Amazon EC2.

Considerações

- Não há caminho de migração de sub-redes somente IPv4 para sub-redes somente IPv6.
- Este exemplo pressupõe que você tenha uma VPC existente com sub-redes públicas e privadas. Para obter mais informações sobre como criar uma VPC para uso com IPv6, consulte the section called “Crie uma VPC”.
- Antes de migrar para IPv6, certifique-se de ter lido os recursos do endereçamento IPv6 para a Amazon VPC: Comparar IPv4 e IPv6.

Conteúdo

Adicionar suporte a IPv6 para sua VPC

A tabela a seguir fornece uma visão geral do processo para habilitar o IPv6 para sua VPC.

Conteúdo

Etapa	Observações
Etapa 1: associar um bloco CIDR IPv6 com a VPC e as sub-redes	Associe um bloco CIDR IPv6 fornecido pela Amazon ou BYOIP à sua VPC e a suas sub-redes.
Etapa 2: atualizar as tabelas de rotas	Atualize as tabelas de rota para encaminhar o tráfego IPv6. Para uma sub-rede pública, crie uma rota que encaminhe todo o tráfego IPv6 da sub-rede para o gateway de Internet. Para uma sub-rede privada, crie uma rota que encaminhe todo o tráfego IPv6 direcionado à Internet da sub-rede para um gateway de Internet somente de saída.
Etapa 3: atualizar as regras do grupo de segurança	Atualize as regras do grupo de segurança de modo a incluir regras para endereços IPv6. Isso permite que o tráfego IPv6 flua para e a partir das instâncias. Se você criou regras personalizadas de ACL de rede para controlar

Etapa	Observações
	o fluxo de tráfego para e a partir da sub-rede, você deve incluir regras para o tráfego IPv6.
Etapa 4: atribuir endereços IPv6 às suas instâncias	Atribua endereços IPv6 às instâncias a partir do intervalo de endereços IPv6 da sub-rede.

Etapa 1: associar um bloco CIDR IPv6 com a VPC e as sub-redes

Você pode associar um bloco CIDR IPv6 com a VPC e, em seguida, associar um bloco CIDR `/64` desse intervalo com cada sub-rede.

Para associar um bloco CIDR IPv6 a uma VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Selecione a VPC.
4. Escolha Ações, Editar CIDRs e depois Adicionar novo CIDR IPv6.
5. Selecione uma das seguintes opções e escolha Selecionar CIDR:
   - Bloco CIDR IPv6 fornecido pela Amazon: use um bloco CIDR IPv6 do grupo de endereços IPv6 da Amazon. Em Grupo de borda da rede, selecione o grupo do qual a AWS anuncia endereços IP.
   - Bloco CIDR IPv6 alocado pelo IPAM: use um bloco CIDR IPv6 a partir de um grupo de IPAM. Escolha o grupo de IPAM e o bloco CIDR IPv6.
   - CIDR IPv6 pertencente a mim: use um bloco CIDR IPv6 do seu grupo de endereços IPv6 (BYOIP). Escolha o grupo de endereços IPv6 e o bloco CIDR IPv6.
6. Escolha Fechar.

Para associar um bloco CIDR IPv6 a uma sub-rede

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Sub-redes.
3. Selecione uma sub-rede.
4. Escolha Ações, Editar CIDRs IPv6 e depois Adicionar CIDR IPv6.

5. Edite o bloco CIDR conforme necessário (por exemplo, substitua `00`).
6. Escolha Salvar.
7. Repita o procedimento para outras sub-redes da VPC.

Para ter mais informações, consulte Blocos CIDR IPv6 da VPC.

Etapa 2: atualizar as tabelas de rotas

Quando você associa um bloco CIDR IPv6 à sua VPC, adicionamos automaticamente uma rota local a cada tabela de rotas da VPC para permitir o tráfego IPv6 nela.

Você deve atualizar as tabelas de rotas das suas sub-redes públicas para permitir que instâncias (como servidores Web) usem o gateway da Internet para tráfego IPv6. Você também deve atualizar as tabelas de rotas de sub-redes privadas para permitir que instâncias (como instâncias de banco de dados) usem um gateway da Internet somente de saída para tráfego IPv6, pois os gateways NAT não são compatíveis com IPv6.

Para atualizar a tabela de rotas de um sub-rede pública

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Sub-redes. Selecione a sub-rede pública. Na guia Tabela de rotas, escolha o ID da tabela de rotas para abrir a respectiva página de detalhes.
3. Selecione a tabela de rotas. Na guia Rotas, escolha Editar rotas.
4. Escolha Adicionar rota. Escolha `::/0` para Destino. Escolha o ID do gateway da Internet para Alvo.
5. Escolha Salvar alterações.

Para atualizar a tabela de rotas de uma sub-rede privada

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Gateways da Internet somente de saída. Escolha Criar um Gateway da Internet somente de saída. Escolha sua VPC em VPC e depois escolha Criar gateway da Internet somente de saída.

   Para ter mais informações, consulte Habilitar o tráfego IPv6 de saída usando gateways da Internet somente de saída.

3. No painel de navegação, escolha Sub-redes. Selecione a sub-rede privada. Na guia Tabela de rotas, escolha o ID da tabela de rotas para abrir a respectiva página de detalhes.
4. Selecione a tabela de rotas. Na guia Rotas, escolha Editar rotas.
5. Escolha Adicionar rota. Escolha `::/0` para Destino. Escolha o ID do gateway da Internet somente de saída para Alvo.
6. Escolha Salvar alterações.

Para ter mais informações, consulte Exemplo de opções de roteamento.

Etapa 3: atualizar as regras do grupo de segurança

Para permitir que as instâncias enviem e recebam tráfego pelo IPv6, é necessário atualizar as regras de grupo de segurança para incluir regras para endereços IPv6. Por exemplo, no exemplo acima, atualize o grupo de segurança do servidor web (`sg-11aa22bb11aa22bb1`) para adicionar regras que permitem HTTP e HTTPS de entrada e acesso SSH a partir de endereços IPv6. Não é necessário fazer alterações nas regras de entrada do seu grupo de segurança de banco de dados. A regra que permite toda a comunicação de `sg-11aa22bb11aa22bb1` inclui a comunicação IPv6.

Para atualizar as regras do grupo de segurança de entrada

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Grupos de segurança e selecione o grupo de segurança do servidor Web.
3. Na guia Regras de entrada, selecione Editar regras de entrada.
4. Para cada regra que permite tráfego IPv4, escolha Adicionar regra e configure-a para permitir o tráfego IPv6 correspondente. Por exemplo, para adicionar uma regra que permite todo o tráfego HTTP via IPv6, escolha HTTP em Tipo e `::/0` em Origem.
5. Quando terminar de adicionar regras, escolha Salvar regras.

Atualizar regras do grupo de segurança de saída

Quando você associa um bloco CIDR IPv6 à sua VPC, adicionamos automaticamente uma regra de saída aos grupos de segurança da VPC que permite todo o tráfego IPv6. No entanto, se você modificou as regras de saída originais para o grupo de segurança, esta regra não será adicionada automaticamente e você deverá adicionar regras de saída equivalentes para o tráfego IPv6.

Atualizar as regras de ACL de rede

Quando você associa um bloco CIDR IPv6 a uma VPC, adicionamos regras automaticamente à ACL de rede padrão para permitir o tráfego IPv6. Porém, se você tiver modificado a ACL de rede padrão ou criado uma ACL de rede personalizada, deverá adicionar manualmente regras para o tráfego IPv6. Para obter mais informações, consulte Adicionar e excluir regras.

Etapa 4: atribuir endereços IPv6 às suas instâncias

Todos os tipos de instância da geração atual oferecem suporte a IPv6. Se o tipo de instância não oferecer suporte a IPv6, redimensione a instância para um tipo compatível antes de poder atribuir um endereço IPv6. O processo a ser usado depende se o novo tipo de instância escolhido é compatível com o atual. Para obter mais informações, consulte Alterar o tipo de instância no Guia do usuário do Amazon EC2. Se você tiver que iniciar uma instância de uma nova AMI para oferecer suporte a IPv6, poderá atribuir um endereço IPv6 à instância durante o lançamento.

Depois de verificar se o tipo de instância oferece suporte ao IPv6, será possível atribuir um endereço IPv6 à instância usando o console do Amazon EC2. O endereço IPv6 é atribuído para a interface de rede primária (por exemplo, eth0) da instância. Para obter mais informações, consulte Atribuir um endereço IPv6 a uma instância no Guia do usuário do Amazon EC2.

É possível conectar-se a uma instância usando seu endereço IPv6. Para obter mais informações, consulte Conectar-se à instância do Linux usando um cliente SSH no Guia do usuário do Amazon EC2.

Se você iniciou sua instância usando uma AMI para uma versão atual do sistema operacional, essa instância está configurada para IPv6. Se você não conseguir efetuar ping em um endereço IPv6 da sua instância, consulte a documentação do seu sistema operacional para configurar o IPv6.

Exemplo de configuração VPC de pilha dupla

Com uma configuração de pilha dupla, você pode usar endereços IPv4 e IPv6 para comunicação entre recursos em sua VPC e recursos pela Internet.

O diagrama a seguir ilustra a arquitetura da VPC. Sua VPC tem uma sub-rede pública e uma sub-rede privada. A VPC e as sub-redes têm um bloco CIDR IPv4 e um bloco CIDR IPv6. Há uma instância do EC2 na sub-rede privada que tem um endereço IPv4 e um endereço IPv6. A instância pode enviar tráfego IPv4 de saída para a Internet usando um gateway NAT e tráfego IPv6 de saída para a Internet usando um gateway da internet somente de saída.

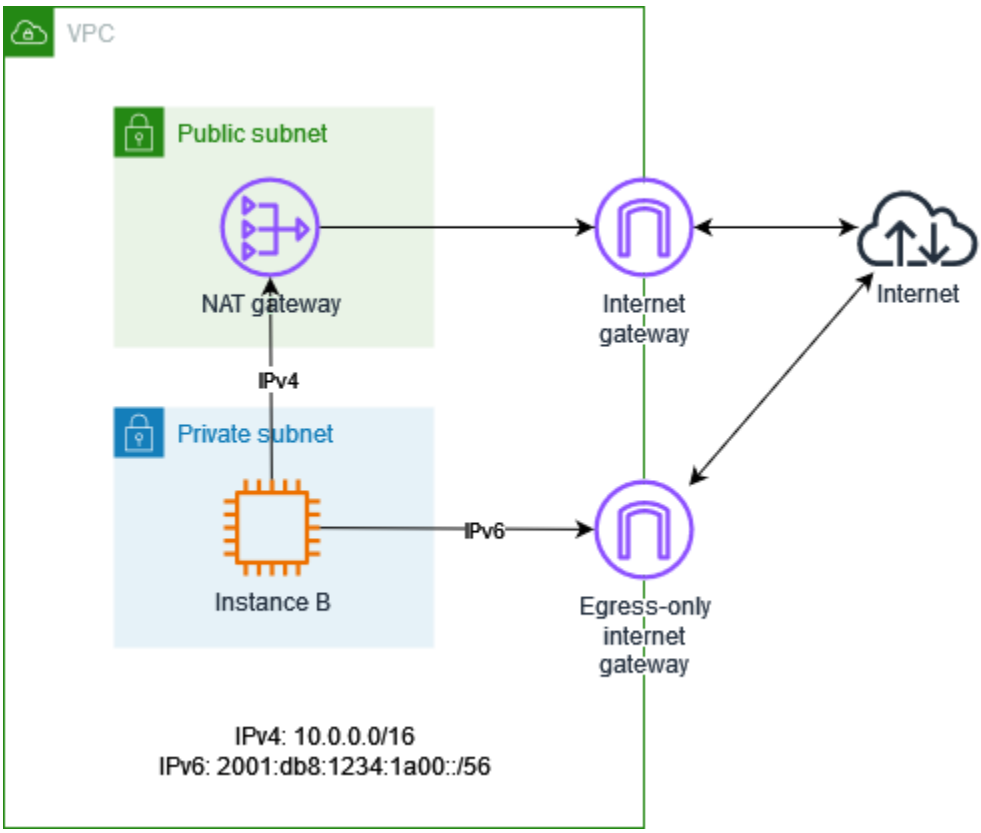


Tabela de rotas para sub-rede pública

Veja a seguir a tabela de rotas para a sub-rede pública. As duas primeiras entradas são as rotas locais. A terceira entrada envia todo o tráfego IPv4 para o gateway da internet. Observe que a quarta entrada é necessária somente se você planeja iniciar instâncias do EC2 com endereços IPv6 na sub-rede pública.

Destino	Alvo
CIDR IPv4 da VPC	local
CIDR IPv6 da VPC	local
0.0.0.0/0	*internet-gateway-id*
::/0	*internet-gateway-id*

Tabela de rotas para a sub-rede privada

Veja a seguir a tabela de rotas da sub-rede privada. As duas primeiras entradas são as rotas locais. A terceira entrada envia todo o tráfego IPv4 para o gateway NAT. A última entrada envia todo o tráfego IPv6 para o gateway da internet apenas de saída.

Destino	Alvo
CIDR IPv4 da VPC	local
CIDR IPv6 da VPC	local
0.0.0.0/0	*nat-gateway-id*
::/0	*egress-only-gateway-id*

Serviços da AWS que oferecem suporte a IPv6

Computadores e dispositivos inteligentes usam endereços IP para se comunicarem entre si pela Internet e por outras redes. À medida que a Internet continua a crescer, também aumenta a necessidade de endereços IP. O formato mais comum para endereços IP é o IPv4. O novo formato para endereços IP é o IPv6, que fornece um espaço de endereçamento maior que o IPv4.

O suporte dos Serviços da AWS a IPv6 inclui suporte à configuração de pilha dupla (IPv4 e IPv6) ou configurações somente IPv6. Por exemplo, uma nuvem privada virtual (VPC) é uma seção isolada logicamente da Nuvem AWS onde é possível iniciar recursos da AWS. Em uma VPC, é possível criar sub-redes que sejam somente IPv4, pilha dupla ou somente IPv6.

Os Serviços da AWS oferecem suporte a acesso através de endpoints públicos. Alguns Serviços da AWS também oferecem suporte ao acesso usando endpoints privados alimentados por AWS PrivateLink. Os Serviços da AWS podem oferecer suporte a IPv6 por meio de seus endpoints privados, mesmo que não ofereçam suporte ao IPv6 por meio de seus endpoints públicos. Os endpoints que oferecem suporte a IPv6 podem responder a consultas de DNS com registros AAAA.

Serviços que oferecem suporte a IPv6

A tabela a seguir lista os Serviços da AWS que oferecem suporte a pilha dupla, suporte somente a IPv6 e endpoints que oferecem suporte a IPv6. Atualizaremos essa tabela à medida que lançarmos suporte adicional para IPv6. Para obter informações específicas sobre como um serviço oferece suporte para IPv6, consulte a documentação desse serviço.

Nome do serviço	Suporte a pilha dupla	Suporte somente a IPv6.	Os endpoints públicos oferecem suporte a IPv6	Os endpoints privados são compatíveis com IPv6 [1]
Amazon API Gateway	Nº	Nº	Nº	Sim
AWS App Mesh	Sim	Sim	Sim	Não
AWS Application Discovery Service	Sim	Não	Sim	Sim
Amazon AppStream 2.0	Sim	Não	Nº	Nº
Amazon Athena	Sim	Não	Sim	Sim
Amazon Aurora	Sim	Não	Sim	Não
AWS Backup	Sim	Não	Sim	Sim
Amazon Braket	Sim	Sim	Sim	Sim
AWS Clean Rooms ML	Sim	Sim	Sim	Sim
AWS Cloud9	Sim	Não	Sim	
AWS Cloud Control API	Sim	Não	Sim	Sim

Nome do serviço	Suporte a pilha dupla	Suporte somente a IPv6.	Os endpoints públicos oferecem suporte a IPv6	Os endpoints privados são compatíveis com IPv6 [1]
Amazon CloudFront	Sim	Não	Nº	
AWS CloudHSM	Sim	Não	Sim	Sim
AWS CloudTrail	Sim	Não	Sim	Sim
Amazon CloudWatch Logs	Sim	Não	Sim	Não
AWS Cloud Map	Sim	Sim	Sim	Sim
AWS Cloud WAN	Sim	Não	Sim	Não
AWS CodeArtifact	Sim	Não	Sim	Sim
Amazon CodeGuru Profiler	Sim	Não	Sim	Sim
Hub de Otimização de Custos da AWS	Sim	Não	Sim	Sim
AWS Elastic Beanstalk	Não	Nº	Sim	Sim
Amazon Cognito	Sim	Não	Sim	

Nome do serviço	Suporte a pilha dupla	Suporte somente a IPv6.	Os endpoints públicos oferecem suporte a IPv6	Os endpoints privados são compatíveis com IPv6 [1]
Amazon Data Firehose	Nº	Nº	Sim	Sim
AWS Database Migration Service	Sim	Não	Nº	Nº
AWS Direct Connect	Sim	Sim	Não	
APIs diretas do Amazon EBS	Sim	Sim	Sim	Sim
Amazon EC2	Sim	Sim	Sim	Não
Amazon ECS	Sim	Não	Nº	Nº
Amazon EKS	P	P	Sim	Sim
Elastic Load Balancing	P	P	Nº	Nº
Amazon ElastiCache	Sim	Sim	Não	Nº
Mensagens sociais dos usuários finais da AWS	Sim	Não	Sim	Não
AWS Entity Resolution	Sim	Não	Sim	Sim

Nome do serviço	Suporte a pilha dupla	Suporte somente a IPv6.	Os endpoints públicos oferecem suporte a IPv6	Os endpoints privados são compatíveis com IPv6 [1]
AWS Fargate	Sim	Não	Nº	Nº
Amazon FSx	Nº	Nº	Sim	Sim
AWS Global Accelerator	Sim	Não	Nº	
AWS Glue	Sim	Não	Nº	Sim
Amazon Managed Grafana [2]	Sim	Não	Sim	Sim
AWS Ground Station [3]	Sim	Não	Sim	Sim
Amazon Inspector	Sim	Sim	Sim	Sim
AWS IoT	Sim	Não	Sim	Não
AWS IoT FleetWise	Sim	Não	Sim	Sim
AWS IoT Wireless	Sim	Não	Sim	Sim
AWS Lake Formation	Não	Nº	Nº	Sim

Nome do serviço	Suporte a pilha dupla	Suporte somente a IPv6.	Os endpoints públicos oferecem suporte a IPv6	Os endpoints privados são compatíveis com IPv6 [1]
AWS Lambda	Sim	Não	Sim	Não
Amazon Lightsail	Sim	Sim	Sim	Não
Amazon Macie	Sim	Não	Sim	Sim
AWS Mainframe Modernization	Sim	Não	Sim	Sim
AWS Network Firewall	Sim	Sim	Não	Nº
Amazon OpenSearch Service	Sim	Não	Sim	Não
Amazon Personalize	Sim	Não	Sim	Sim
Amazon Pinpoint	Sim	Não	Sim	Não
Amazon Polly	Sim	Não	Sim	Sim
Conector para SCEP da AWS Private CA	Sim	Sim	Sim	Sim
AWS PrivateLink	Sim	Sim	Sim	

Nome do serviço	Suporte a pilha dupla	Suporte somente a IPv6.	Os endpoints públicos oferecem suporte a IPv6	Os endpoints privados são compatíveis com IPv6 [1]
Amazon Managed Service para Prometheus	Sim	Não	Sim	Sim
Amazon RDS	Sim	Não	Sim	Não
Explorador de recursos da AWS	Sim	Não	Sim	
Amazon Route 53	Sim	Sim	Não	
Amazon S3	Sim	Não	Sim	Não
AWS Secrets Manager	Sim	Não	Sim	Não
AWS Shield	Sim	Sim	Não	
AWS Site-to-Site VPN	Sim	Não	Sim	Não
AWS Transit Gateway	Sim	Não	Sim	Não
Amazon Translate	Sim	Sim	Sim	Sim
Amazon VPC	Sim	Sim	Sim	Não

Nome do serviço	Suporte a pilha dupla	Suporte somente a IPv6.	Os endpoints públicos oferecem suporte a IPv6	Os endpoints privados são compatíveis com IPv6 [1]
AWS WAF	Sim	Sim	Não	
Amazon WorkSpaces	Sim	Não	Nº	Nº
AWS X-Ray	Sim	Não	Sim	Sim

[1] Uma célula vazia indica que o serviço não tem integração com o AWS PrivateLink.

[2] Esta entrada representa o suporte IPv6 para operações de gerenciamento de espaços de trabalho do Grafana, como a atualização de espaços de trabalho e as permissões de espaço de trabalho. Não há suporte para o endereço IPv6 para operações gerais de espaços de trabalho do Grafana, como criar e editar painéis ou consultar fontes de dados.

[3] Esta entrada representa o suporte a IPv6 para operações do ambiente de gerenciamento do AWS Ground Station, como chamar a API do AWS Ground Station. Não há suporte ao IPv6 pelo plano de dados do AWS Ground Station, por exemplo, a entrega de dados para uma instância do Amazon EC2 usando IPv6.

Suporte adicional a IPv6

Computação

- O Amazon EC2 oferece suporte à execução de instâncias baseadas no Nitro System em sub-redes somente IPv6.
- O Amazon EC2 fornece endpoints do IPv6 para o Serviço de metadados da instância (IMDS) e o Serviço de Sincronização Temporal da Amazon.

Rede e entrega de conteúdo

- A Amazon VPC oferece suporte à criação de sub-redes somente IPv6.

- A Amazon VPC ajuda os recursos IPv6 da AWS a se comunicarem com recursos IPv4 ao oferecer suporte ao DNS64 em suas sub-redes e ao NAT64 em seus gateways NAT.

Segurança, identidade e conformidade

- O AWS Identity and Access Management (IAM) oferece suporte ao endereços IPv6 em políticas baseadas em identidade do IAM.
- O Amazon Macie oferece suporte a endereços IPv6 em informações de identificação pessoal (PII).

Gerenciamento e governança

- Os registros do AWS CloudTrail incluem informações IPv6 de origem.
- A AWS CLI v2oferece suporte a download sobre conexões IPv6 para clientes somente IPv6.

Saiba mais

- IPv6 na AWS
- Arquiteturas de referência da Amazon VPC de pilha dupla e somente IPv6 (PDF)

Configurar uma nuvem privada virtual

A Amazon Virtual Private Cloud (VPC) é um bloco fundamental do ecossistema da AWS, permitindo a você provisionar redes virtuais isoladas na Nuvem . Ao criar sua própria VPC, você obtém controle total sobre o ambiente de rede, incluindo a capacidade de definir intervalos de endereços IP, sub-redes, tabelas de roteamento e opções de conectividade.

Sua conta da AWS contém uma VPC padrão para cada região da AWS. Essa VPC padrão é pré-configurada com opções que a tornam uma alternativa conveniente para iniciar rapidamente seus recursos. No entanto, a VPC padrão nem sempre está alinhada às suas necessidades de rede de longo prazo. É aqui que a criação de VPCs adicionais pode ser vantajosa.

A criação de VPCs adicionais oferece várias vantagens em relação à VPC padrão provisionada com cada nova conta da AWS. Com uma VPC autogerenciada, você pode arquitetar a topologia da rede para se alinhar com precisão aos seus requisitos específicos, seja implementando uma aplicação de várias camadas, conectando-se a recursos on-premises ou segregando workloads por departamento ou unidade de negócios.

Além disso, a criação de várias VPCs pode permitir maior segurança e isolamento entre suas diferentes aplicações ou unidades de negócios. Cada VPC atua como uma rede virtual separada, permitindo que você aplique políticas de segurança, controles de acesso e configurações de roteamento distintas personalizadas para cada ambiente.

Em última análise, a decisão de usar a VPC padrão ou criar uma (ou mais) VPCs personalizadas deve ser baseada em seus requisitos específicos de aplicações, necessidades de segurança e metas de escalabilidade de longo prazo. Investir tempo para projetar cuidadosamente sua infraestrutura de VPC pode render dividendos na forma de uma base de rede em nuvem robusta, segura e adaptável.

Conteúdo

- Conjuntos de opções DHCP no Amazon VPC
- Atributos de DNS para sua VPC
- Uso de endereço de rede para sua VPC
- Compartilhar as sub-redes da sua VPC com outras contas
- Estender uma VPC para uma zona local, zona Wavelength ou Outpost
- Excluir a VPC:
- Gerar infraestrutura como código com base nas ações do seu console VPC usando o Console-to-Code

Conceitos básicos da VPC

Uma VPC abrange todas as zonas de disponibilidade em uma região. Depois de criar uma VPC, você pode adicionar uma ou mais sub-redes em cada zona de disponibilidade. Para ter mais informações, consulte Sub-redes.

Conteúdo

- Intervalo de endereços IP da VPC
- Diagrama da VPC
- Recursos da VPC

Intervalo de endereços IP da VPC

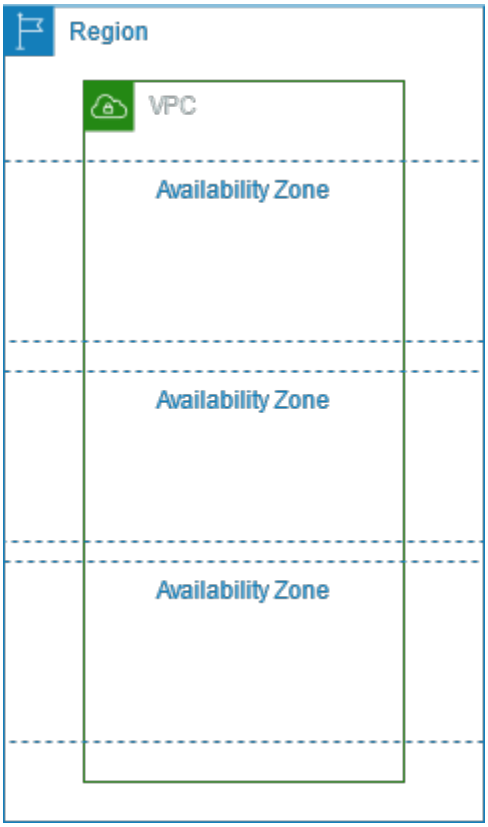
Na criação de uma VPC, você especifica seus endereços IP da seguinte maneira:

- Somente IPv4: a VPC tem um bloco CIDR IPv4, mas não um bloco CIDR IPv6.
- Pilha dupla: a VPC tem um bloco CIDR IPv4 e um bloco CIDR IPv6.

Para ter mais informações, consulte Endereçamento IP para suas VPCs e sub-redes.

Diagrama da VPC

O diagrama a seguir mostra uma VPC sem recursos adicionais de VPC. Para obter exemplos de configurações de VPC, consulte Exemplos.



Recursos da VPC

Cada VPC vem automaticamente com os seguintes recursos:

- Conjunto padrão de opções de DHCP
- ACL de rede padrão
- Grupo de segurança padrão
- Tabela de rotas principal

É possível criar os seguintes recursos para sua VPC:

- Network ACLs
- Tabelas de rotas personalizadas
- Grupos de segurança
- gateway da Internet
- Gateways NAT

Opções de configuração da VPC

Também é possível especificar as seguintes opções de configuração ao criar uma VPC.

Zonas de disponibilidade

Data centers distintos com energia, redes e conectividade redundantes em uma região da AWS. É possível usar várias AZs para operar aplicações e bancos de dados de produção com níveis superiores de alta disponibilidade, tolerância a falhas e escalabilidade ao que seria possível com um só data center. Se particionar entre AZs suas aplicações executadas em sub-redes, você terá níveis melhores de isolamento e proteção contra problemas como falta de energia elétrica, raios, tornados e terremotos.

Blocos CIDR

Você deve especificar intervalos de endereços IP para sua VPC e sub-redes. Para ter mais informações, consulte Endereçamento IP para suas VPCs e sub-redes.

Opções de DNS

Se você precisar de nomes de host de DNS IPv4 públicos para as instâncias do EC2 executadas em suas sub-redes, habilite as duas opções de DNS. Para ter mais informações, consulte Atributos de DNS para sua VPC.

- Habilitar nomes de host de DNS: as instâncias do EC2 iniciadas na VPC recebem nomes de host de DNS públicos que correspondem aos seus endereços IPv4 públicos.
- Habilitar resolução de DNS: a resolução de DNS para nomes de host de DNS privados é fornecida para a VPC pelo servidor Amazon DNS, chamado Route 53 Resolver.

Gateway da Internet

Conecta sua VPC à Internet. As instâncias em uma sub-rede pública podem acessar a Internet porque a tabela de rotas de sub-redes contém uma rota que envia tráfego destinado à Internet para o gateway da Internet. Se um servidor não precisar ser acessado diretamente pela Internet, você não deve implantá-lo em uma sub-rede pública. Para obter mais informações, consulte Gateways da Internet.

Nome

Os nomes que você especifica para a VPC e os outros recursos da VPC são usados para criar as tags de nome. Se você usar o recurso de geração automática de tags de nome no console, os valores das tags terão o formato *nome*-*recurso*.

Gateways NAT

Permite que instâncias em uma sub-rede privada enviem tráfego para a Internet, mas impede que recursos na Internet se conectem às instâncias. No ambiente de produção, recomendamos implantar um gateway NAT em cada AZ ativa. Para obter mais informações, consulte Gateways de NAT.

Tabelas de rotas

Contém um conjunto de regras, chamado de rotas, que determinam para onde o tráfego de rede de sua sub-rede ou gateway é direcionado. Para obter mais informações, consulte Tabelas de rotas.

Sub-redes

Um intervalo de endereços IP na VPC. É possível iniciar recursos da AWS, como instâncias do EC2, nas suas sub-redes. Cada sub-rede rese inteiramente dentro de uma zona de disponibilidade. Ao iniciar as instâncias em ao menos duas zonas de disponibilidade, é possível proteger suas aplicações contra a falha de uma única zona de disponibilidade.

Uma sub-rede pública tem uma rota direta para um gateway da Internet. Os recursos em uma sub-rede pública podem acessar a Internet pública. Uma sub-rede privada não tem uma rota de direta para um gateway da Internet. Os recursos em uma sub-rede privada exigem um outro componente, como um dispositivo NAT, para acessar a Internet pública.

Para obter mais informações, consulte Sub-redes.

Locação

Essa opção define se as instâncias do EC2 que você executa na VPC serão executadas em hardware compartilhado com outras Contas da AWS ou em hardware dedicado somente para seu uso. Se você escolher `Default` para a locação da VPC, as instâncias do EC2 executadas nessa VPC usarão o atributo de locação especificado na execução da instância. Para obter mais informações, consulte Iniciar uma instância usando parâmetros definidos no Guia do usuário do Amazon EC2. Se você escolher a locação da VPC para ser `Dedicated`, as instâncias sempre serão executadas como Instâncias dedicadas no hardware dedicado ao seu uso. Se estiver usando o AWS Outposts, o seu Outpost vai requerer conectividade privada; você deve usar a locação `Default`.

VPCs padrão

Quando começa a usar o Amazon VPC, você tem uma VPC padrão em cada região da AWS. Uma VPC padrão vem com uma sub-rede pública em cada zona de disponibilidade, um gateway da Internet e configurações para habilitar a resolução de DNS. Portanto, você pode começar a iniciar imediatamente instâncias do Amazon EC2 em uma VPC padrão. Você também pode usar serviços como Elastic Load Balancing, Amazon RDS e Amazon EMR em sua VPC padrão.

Uma VPC padrão é adequada para começar a operar rapidamente e iniciar instâncias públicas, como um blog ou um site simples. Você pode modificar os componentes da VPC padrão conforme necessário.

Você também pode adicionar sub-redes à VPC padrão. Para ter mais informações, consulte the section called “Criar uma sub-rede”.

Conteúdo

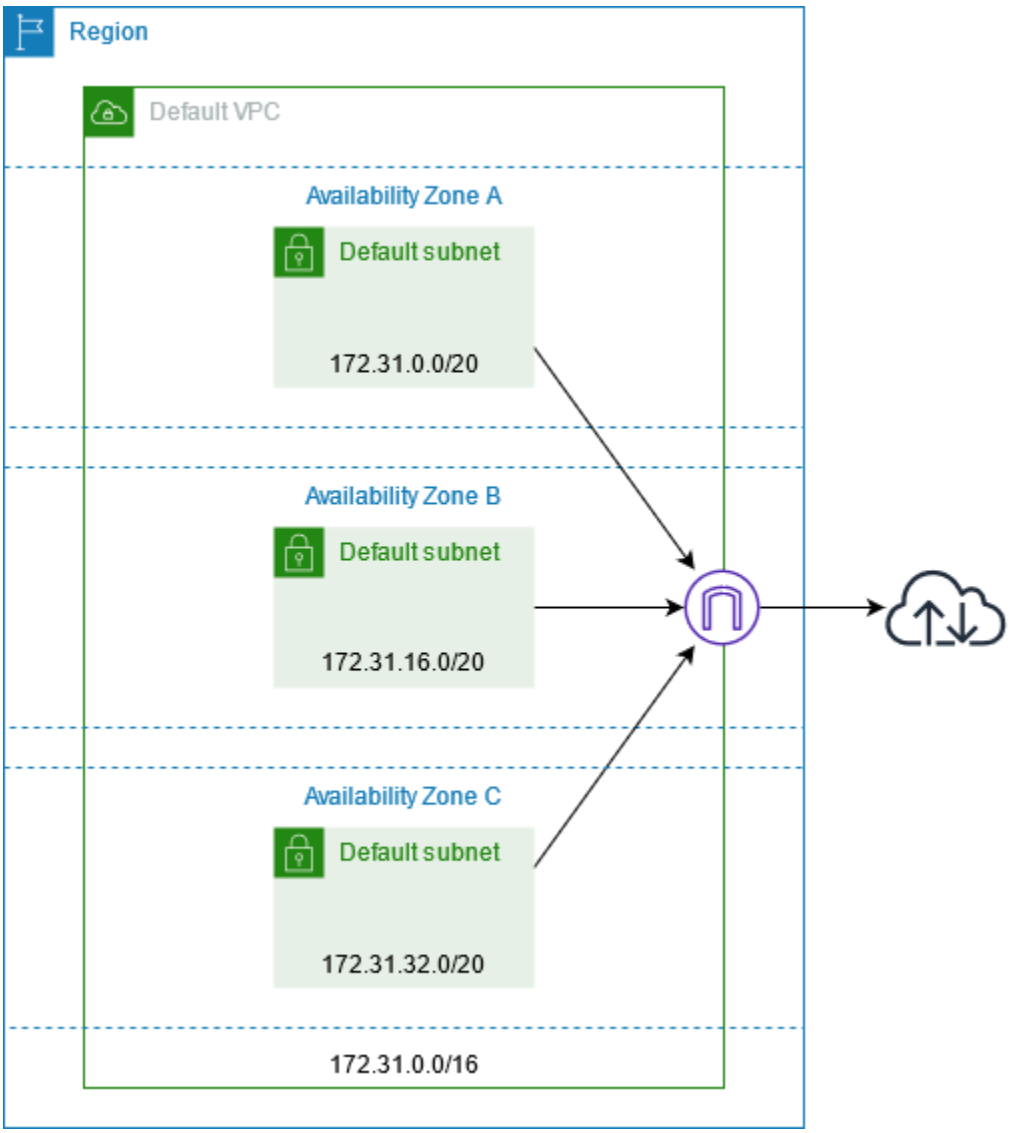
Componentes da VPC padrão

Quando criamos uma VPC padrão, nós realizamos as seguintes etapas para configurá-la:

- Crie uma VPC com um bloco CIDR IPv4 de tamanho `/16` (`172.31.0.0/16`). Isso fornece até 65.536 endereços IPv4 privados.
- Crie uma sub-rede padrão de tamanho `/20` em cada zona de disponibilidade. Isso fornece até 4.096 endereços por sub-rede, alguns dos quais são reservados para nosso uso.
- Crie um gateway da internet e conecte-o à VPC padrão.
- Crie uma rota na tabela de rotas que direcione todo o tráfego (`0.0.0.0/0`) para o gateway da Internet.
- Criar um security group padrão e associá-lo à sua VPC padrão.
- Criar uma lista de controle de acesso de rede padrão e associá-la à sua VPC padrão.
- Associar o conjunto padrão de opções de DHCP da sua conta da AWS a sua VPC padrão.

> **Note**
>
> - A Amazon cria os recursos acima em seu nome. As políticas do IAM não se aplicam a essas ações porque você não as executa. Por exemplo, se você tiver uma política do IAM que nega a possibilidade de chamar CreateInternetGateway, e você chamar CreateDefaultVpc, o gateway da Internet na VPC padrão ainda será criado. Para impedir que a Amazon crie um gateway da Internet, é necessário negar as permissões CreateDefaultVpc e CreateInternetGateway.
> - Para bloquear todo o tráfego de e para os gateways da Internet na sua conta, consulte Bloquear o acesso público a VPCs e sub-redes.

A figura a seguir ilustra os principais componentes que configuramos para uma VPC padrão.



A tabela a seguir mostra as rotas na tabela de rotas principal para a VPC padrão.

Destino	Destino
172.31.0.0/16	local
0.0.0.0/0	*internet_gateway_id*

Você pode usar uma VPC padrão como usaria qualquer outra VPC:

- Adicionar mais sub-redes não padrão.
- Modificar a tabela de rotas principal.

- Adicionar mais tabelas de rotas.
- Associar security groups adicionais.
- Atualizar as regras do security group padrão.
- Adicione conexões do AWS Site-to-Site VPN.
- Adicione mais blocos CIDR IPv4.
- Acesse VPCs em uma região remota usando um gateway Direct Connect. Para obter informações sobre opções do gateway Direct Connect, consulte Gateways Direct Connect no Manual do usuário do AWS Direct Connect.

Você pode usar uma sub-rede padrão da mesma forma como usaria qualquer outra sub-rede: adicionar tabelas de rotas personalizadas e definir Network ACLs. Você também pode especificar uma sub-rede padrão específica ao executar uma instância do EC2.

É possível associar, opcionalmente, um bloco CIDR IPv6 à VPC padrão.

Sub-redes padrão

Por padrão, uma sub-rede padrão é uma sub-rede pública, porque a tabela de rotas principal envia o tráfego da sub-rede destinado para a internet para o gateway da internet. É possível transformar uma sub-rede padrão em uma sub-rede privada removendo a rota do destino 0.0.0.0/0 para o gateway da internet. No entanto, se você fizer isso, nenhuma instância do EC2 executada nessa sub-rede poderá acessar a Internet.

As instâncias que você executa em uma sub-rede padrão recebem um endereço IPv4 público e um endereço IPv4 privado, e os dois nomes de host DNS público e privado. As instâncias iniciadas em uma sub-rede não padrão em uma VPC padrão não recebem um endereço IPv4 público nem um nome de host DNS. É possível alterar o comportamento do endereçamento IP público padrão da sub-rede. Para obter mais informações, consulte Modificar os atributos de endereçamento IP da sua sub-rede.

Periodicamente, a AWS poderá adicionar uma nova zona de disponibilidade a uma região. Na maioria dos casos, criaremos automaticamente uma nova sub-rede padrão nessa zona de disponibilidade para sua VPC padrão dentro de alguns dias. No entanto, se você tiver feito modificações na VPC padrão, não adicionaremos uma nova sub-rede padrão. Se quiser uma sub-rede padrão para a nova zona de disponibilidade, você mesmo poderá criar uma. Para ter mais informações, consulte Criar uma sub-rede padrão.

Trabalhar com a VPC padrão e suas sub-redes padrão

Esta seção descreve como trabalhar com VPCs e sub-redes padrão.

Conteúdo

Visualizar a VPC e as sub-redes padrão

É possível visualizar a VPC e as sub-redes padrão usando o console da Amazon VPC ou a linha de comando.

Para visualizar a VPC e as sub-redes padrão usando o console da

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Na coluna Default VPC, procure um valor de Yes. Anote o ID da VPC padrão.
4. No painel de navegação, escolha Sub-redes.
5. Na barra de pesquisa, digite o ID da VPC padrão. As sub-redes retornadas são sub-redes na VPC padrão.
6. Para verificar quais sub-redes são sub-redes padrão, procure um valor de Yes na coluna Default Subnet.

Para descrever a VPC padrão usando a linha de comando

- Use describe-vpcs (AWS CLI)
- Use Get-EC2Vpc (AWS Tools for Windows PowerShell)

Use os comandos com o filtro `isDefault` e defina o valor do filtro como `true`.

Para descrever as sub-redes padrão usando a linha de comando

- Use describe-subnets (AWS CLI)

- Use Get-EC2Subnet (AWS Tools for Windows PowerShell)

Use os comandos com o filtro `vpc-id` e defina o valor do filtro como o ID da VPC padrão. Na saída, o campo `DefaultForAz` é definido como `true` para as sub-redes padrão.

Criar uma VPC padrão

Se excluir a VPC padrão, você poderá criar uma nova. Você não pode recuperar um VPC padrão anterior excluída e não pode marcar uma VPC não padrão existente como uma VPC padrão.

Quando você cria uma VPC padrão, ela é criada com os componentes padrão de uma VPC padrão, incluindo uma sub-rede padrão em cada zona de disponibilidade. Você não pode especificar seus próprios componentes. Os blocos CIDR da sub-rede da nova VPC padrão não podem ser mapeados para as mesmas zonas de disponibilidade que a VPC padrão anterior. Por exemplo, se a sub-rede com o bloco CIDR `172.31.0.0/20` foi criada em `us-east-2a` na VPC padrão anterior, ela poderá ser criada em `us-east-2b` na nova VPC padrão.

Se você já tem uma VPC padrão na região, não pode criar outra.

Para criar uma VPC padrão usando o console da

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Escolha Actions, Create Default VPC.
4. Escolha Criar. Feche a tela de confirmação.

Para criar uma VPC padrão usando a linha de comando

Você pode usar o comando create-default-vpc da AWS CLI. Esse comando não tem nenhum parâmetro de entrada.

```
aws ec2 create-default-vpc
```

A seguir está um exemplo de saída.

```
{
    "Vpc": {
        "VpcId": "vpc-3f139646",
```

```
        "InstanceTenancy": "default",
        "Tags": [],
        "Ipv6CidrBlockAssociationSet": [],
        "State": "pending",
        "DhcpOptionsId": "dopt-61079b07",
        "CidrBlock": "172.31.0.0/16",
        "IsDefault": true
    }
}
```

Como alternativa, você pode usar o comando New-EC2DefaultVpc do Tools for Windows PowerShell ou a ação CreateDefaultVpc da API do Amazon EC2.

Criar uma sub-rede padrão

> **Note**
>
> Não é possível criar uma sub-rede padrão usando o AWS Management Console.

Você pode criar uma sub-rede padrão em uma zona de disponibilidade que não tenha uma. Por exemplo, talvez você queira criar uma sub-rede padrão se tiver excluído uma sub-rede padrão ou se a AWS tiver adicionado uma nova zona de disponibilidade e não tiver criado automaticamente uma sub-rede padrão para essa zona na VPC padrão.

Quando você cria uma sub-rede padrão, ela vem com um bloco CIDR IPv4 de tamanho `/20` no espaço contíguo seguinte disponível na VPC padrão. As seguintes regras se aplicam:

- Você não pode especificar o bloco CIDR sozinho.
- Você não pode restaurar uma sub-rede padrão anterior que tenha excluído.
- Você pode ter somente uma sub-rede padrão por zona de disponibilidade.
- Não é possível criar uma sub-rede padrão em uma VPC não padrão.

Se a sua VPC padrão não tiver espaço de endereço suficiente para criar um bloco CIDR de tamanho `/20`, a solicitação falhará. Se você precisar de mais espaço de endereço, pode adicionar um bloco CIDR IPv4 à sua VPC.

Se você tiver associado um bloco CIDR IPv6 à VPC padrão, a nova sub-rede padrão não receberá automaticamente um bloco CIDR IPv6. Em vez disso, você pode associar um bloco CIDR IPv6 à

sub-rede padrão depois de criá-la. Para ter mais informações, consulte Adicionar ou remover um bloco CIDR IPv6 da sua sub-rede.

Como criar uma sub-rede padrão usando a AWS CLI

Use o comando create-default-subnet da AWS CLI e especifique a zona de disponibilidade na qual a sub-rede deve ser criada.

```
aws ec2 create-default-subnet --availability-zone us-east-2a
```

A seguir está um exemplo de saída.

```
{
    "Subnet": {
        "AvailabilityZone": "us-east-2a",
        "Tags": [],
        "AvailableIpAddressCount": 4091,
        "DefaultForAz": true,
        "Ipv6CidrBlockAssociationSet": [],
        "VpcId": "vpc-1a2b3c4d",
        "State": "available",
        "MapPublicIpOnLaunch": true,
        "SubnetId": "subnet-1122aabb",
        "CidrBlock": "172.31.32.0/20",
        "AssignIpv6AddressOnCreation": false
    }
}
```

Para obter mais informações sobre a configuração da AWS CLI, consulte o Manual do usuário da AWS Command Line Interface.

Como alternativa, é possível usar o comando New-EC2DefaultSubnet do Tools for Windows PowerShell ou a ação CreateDefaultSubnet da API do Amazon EC2.

Excluir sub-redes e VPC padrão

É possível excluir uma sub-rede padrão ou uma VPC padrão, assim como qualquer outra sub-rede ou VPC. No entanto, se você excluir suas sub-redes padrão ou a VPC padrão, deverá especificar explicitamente uma sub-rede em uma de suas VPCs ao iniciar instâncias. Se você não tiver outra VPC, será preciso criar uma VPC com uma sub-rede em ao menos uma zona de disponibilidade. Para ter mais informações, consulte Crie uma VPC.

Se excluir a VPC padrão, você poderá criar uma nova. Para obter mais informações, consulte Criar uma VPC padrão.

Se excluir uma sub-rede padrão, você poderá criar uma nova. Para ter mais informações, consulte Criar uma sub-rede padrão. Para garantir que o comportamento da nova sub-rede padrão seja o desejável, modifique o atributo da sub-rede para atribuir endereços IP públicos às instâncias executadas naquela sub-rede. Para obter mais informações, consulte Modificar os atributos de endereçamento IP da sua sub-rede. Você pode ter somente uma sub-rede padrão por zona de disponibilidade. Não é possível criar uma sub-rede padrão em uma VPC não padrão.

Crie uma VPC

Use os procedimentos a seguir para criar uma nuvem privada virtual (VPC). Uma VPC deve ter recursos adicionais, como sub-redes, tabelas de rotas e gateways, antes que você possa criar recursos da AWS na VPC.

Conteúdo

- Criar uma VPC e outros recursos de VPC
- Criar apenas uma VPC
- Criar uma VPC usando a AWS CLI

Para obter informações sobre como modificar VPCs, consulte the section called “Adicionar ou remover bloco CIDR”.

Criar uma VPC e outros recursos de VPC

Use o procedimento a seguir para criar uma VPC, mais os recursos adicionais de VPC necessários para executar sua aplicação, como sub-redes, tabelas de rotas, gateways da Internet e gateways NAT. Para obter exemplos de configurações de VPC, consulte Exemplos.

Para criar uma VPC, sub-redes e outros recursos de VPC usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel da VPC, escolha Criar VPC.
3. Em Resources to create (Recursos a serem criados), escolha VPC and more (VPC e mais).

4. Mantenha a opção Geração automática de tags de nome selecionada para criar tags de nome para os recursos da VPC ou desmarque-a para fornecer suas próprias tags de nome para os recursos da VPC.
5. Em Bloco CIDR IPv4, digite uma faixa de endereços IPv4 para sua VPC. Uma VPC deve ter uma faixa de endereços IPv4.
6. (Opcional) Para oferecer suporte ao tráfego de IPv6, escolha Bloco CIDR IPv6, Bloco CIDR IPv6 fornecido pela Amazon.
7. Escolha uma opção de Locação. Essa opção define se as instâncias do EC2 que você executa na VPC serão executadas em hardware compartilhado com outras Contas da AWS ou em hardware dedicado somente para seu uso. Se você escolher que a locação da VPC seja `Default`, as instâncias do EC2 executadas nessa VPC usarão o atributo de locação especificado quando você executar a instância. Para obter mais informações, consulte Iniciar uma instância usando parâmetros definidos no Guia do usuário do Amazon EC2. Se você escolher a locação da VPC para ser `Dedicated`, as instâncias sempre serão executadas como Instâncias dedicadas no hardware dedicado ao seu uso. Se estiver usando o AWS Outposts, o seu Outpost vai requerer conectividade privada; você deve usar a locação `Default`.
8. Em Número de zonas de disponibilidade (AZs), recomendamos que você provisione sub-redes em pelo menos duas zonas de disponibilidade para um ambiente de produção. Para escolher as AZs para suas sub-redes, expanda Personalizar AZs. Caso contrário, deixe a AWS escolhê-los para você.
9. Para configurar suas sub-redes, escolha valores para Número de sub-redes públicas e Número de sub-redes privadas. Para escolher os intervalos de endereços IP para suas sub-redes, expanda Personalizar blocos CIDR de sub-redes. Caso contrário, deixe a AWS escolhê-los para você.
10. (Opcional) Se os recursos em uma sub-rede privada precisarem de acesso à Internet pública via IPv4, em gateways NAT, escolha o número de AZs nos quais criar gateways NAT. Em produção, recomendamos que você implante um gateway NAT em cada AZ com recursos que precisem de acesso à Internet pública. Observe que existe um custo associado aos gateways NAT. Para ter mais informações, consulte Preços de gateways NAT.
11. (Opcional) Se os recursos em uma sub-rede privada precisarem de acesso à Internet pública via IPv6, escolha Sim em Gateway da Internet somente de saída.
12. (Opcional) Se você precisar acessar o Amazon S3 diretamente da sua VPC, escolha Endpoints da VPC, Gateway do S3. Isso cria um endpoint da VPC de gateway para o Amazon S3. Para obter mais informações, consulte Gateway endpoints no Guia do AWS PrivateLink.

13. (Opcional) Em opções de DNS, as duas opções de resolução de nomes de domínio estão habilitadas por padrão. Se o padrão não atender às suas necessidades, você poderá desabilitar essas opções.
14. (Opcional) Para adicionar uma tag à sua VPC, expanda Tags adicionais, escolha Adicionar nova tag e digite uma chave de tag e um valor de tag.
15. No painel Visualização, é possível visualizar as relações entre os recursos da VPC que você configurou. Linhas sólidas representam relações entre recursos. As linhas pontilhadas representam o tráfego de rede para gateways NAT, gateway da Internet e endpoints de gateway. Após criar a VPC, será possível visualizar os recursos em sua VPC nesse formato a qualquer momento usando a guia Mapa de recursos. Para ter mais informações, consulte Visualizar os recursos em sua VPC.
16. Ao concluir a configuração da sua VPC, escolha Criar VPC.

Criar apenas uma VPC

Siga o procedimento abaixo para criar uma VPC sem recursos de VPC adicionais usando o console da Amazon VPC.

Para criar uma VPC sem recursos de VPC adicionais usando o console

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel da VPC, escolha Criar VPC.
3. Em Recursos a serem criados, escolha Somente VPC.
4. (Opcional) Em Tag de nome, insira um nome para a sua VPC. Ao fazer isso, é criada uma tag com a chave `Name` e o valor especificado.
5. Em IPv4 CIDR block (Bloco CIDR IPv4), execute uma das seguintes ações:
   - Escolha Entrada manual de CIDR IPv4 e insira um intervalo de endereços IPv4 para a sua VPC.
   - Escolha Bloco CIDR IPv4 alocado pelo IPAM, selecione seu grupo de endereços IPV4 do IP Address Manager (IPAM) da Amazon VPC e uma máscara de rede. O tamanho do bloco CIDR é limitado pelas regras de alocação no grupo do IPAM. O IPAM é um recurso de VPC que facilita o planejamento, o rastreamento e o monitoramento de endereços IP de suas workloads da AWS. Para obter mais informações, consulte o Manual do usuário do Amazon VPC IPAM.

Se você estiver usando o IPAM para gerenciar seus endereços IP, recomendamos que você escolha essa opção. Caso contrário, o bloco CIDR que você especificar para sua VPC pode se sobrepor a uma alocação de CIDR do IPAM.

6. (Opcional) Para criar uma VPC de pilha dupla, especifique um intervalo de endereços IPv6 para sua VPC. Em IPv6 CIDR block (Bloco CIDR IPv6), execute uma das seguinte ações:

   - Escolha o bloco CIDR IPv6 alocado pelo IPAM se estiver usando o Amazon VPC IP Address Manager e quiser provisionar um CIDR IPv6 de um grupo do IPAM. Se você usar o bloco CIDR com o endereço IPv6 alocado pelo IPAM para provisionar CIDRs com o endereço IPv6 para as VPCs, você obterá o benefício de CIDRs com o endereço IPv6 contíguos para a criação de VPCs. Os CIDRs alocados de forma contígua se tratam de CIDRs que são alocados sequencialmente. Esses CIDRs possibilitam simplificar as regras de segurança e de rede. Além disso, os CIDRs com o endereço IPv6 podem ser agregados em uma única entrada em componentes de rede e de segurança, como listas de controle de acesso, tabelas de rotas, grupos de segurança e firewalls.

     Você tem duas opções para provisionar um intervalo de endereços de IP para a VPC no bloco CIDR:

     - Comprimento da máscara de rede: Escolha essa opção para selecionar um comprimento de máscara de rede para o CIDR. Execute um destes procedimentos:
       - Se um comprimento de máscara de rede padrão estiver previamente escolhido para o grupo do IPAM, é possível optar por Padrão" para o comprimento de máscara de rede do IPAM e utilizar o comprimento padrão estabelecido para o grupo do IPAM pelo administrador do IPAM. Para informações detalhadas sobre a regra opcional de alocação de comprimento de máscara de rede padrão, consulte o Guia do usuário do IPAM do Amazon VPC na seção sobre a criação de um grupo de IPv6 regional.
       - Caso não haja um comprimento de máscara de rede padrão definido para o grupo do IPAM, é necessário selecionar um comprimento de máscara de rede que seja mais específico que o comprimento da máscara de rede do CIDR associado ao grupo do IPAM. Por exemplo, se o CIDR do grupo do IPAM for /50, você poderá escolher um comprimento de máscara de rede entre /52 e /60 para a VPC. Os comprimentos possíveis da máscara de rede estão entre /44 e /60 em incrementos de /4.
     - Selecione um CIDR: escolha essa opção para inserir manualmente um endereço IPv6. Você só pode escolher um comprimento de máscara de rede que seja mais específico do que o comprimento da máscara de rede do CIDR do grupo do IPAM. Por exemplo, se o CIDR do

grupo do IPAM for /50, você poderá escolher um comprimento de máscara de rede entre /52 e /60 para a VPC. Os possíveis comprimentos de máscara de rede IPv6 estão entre /44 e /60 em incrementos de /4.

- Escolha Bloco CIDR IPv6 fornecido pela Amazon para solicitar um bloco CIDR IPv6 do grupo de endereços IPv6 da Amazon. Em Network Border Group (Grupo de borda de rede), selecione o grupo do qual a AWS anuncia endereços IP. A Amazon fornece um tamanho de bloco CIDR IPv6 fixo de /56.
- Escolha CIDR IPv6 de minha propriedade para provisionar um CIDR IPv6 que você já trouxe para o AWS. Para obter mais informações sobre como trazer seus próprios intervalos de endereços de IP para a AWS, consulte Traga seus próprios endereços IP (BYOIP) no Guia do usuário do Amazon EC2. Você pode provisionar um intervalo de endereços IP para a VPC usando as seguintes opções para o bloco CIDR:
  - Sem preferência: Escolha essa opção para usar o comprimento da máscara de rede de /56.
  - Selecionar um CIDR: escolha essa opção para inserir manualmente um endereço IPv6 e escolher um comprimento de máscara de rede que seja mais específico do que o tamanho do CIDR do BYOIP. Por exemplo, se o CIDR do grupo BYOIP for /50, você poderá escolher um comprimento de máscara de rede entre /52 e /60 para o VPC. Os possíveis comprimentos de máscara de rede IPv6 estão entre /44 e /60 em incrementos de /4.

7. (Opcional) Escolha uma opção de Locação. Essa opção define se as instâncias do EC2 que você executa na VPC serão executadas em hardware compartilhado com outras Contas da AWS ou em hardware dedicado somente para seu uso. Se você escolher `Default` para a locação da VPC, as instâncias do EC2 executadas nessa VPC usarão o atributo de locação especificado na execução da instância. Para obter mais informações, consulte Iniciar uma instância usando parâmetros definidos no Guia do usuário do Amazon EC2. Se você escolher a locação da VPC para ser `Dedicated`, as instâncias sempre serão executadas como Instâncias dedicadas no hardware dedicado ao seu uso. Se estiver usando o AWS Outposts, o seu Outpost vai requerer conectividade privada; você deve usar a locação `Default`.
8. (Opcional) Para adicionar uma tag à sua VPC, escolha Adicionar nova tag e insira uma chave de tag e um valor de tag.
9. Escolha Criar VPC.
10. Após criar uma VPC, você pode adicionar sub-redes. Para ter mais informações, consulte Criar uma sub-rede.

Criar uma VPC usando a AWS CLI

O procedimento a seguir contém exemplos de comandos da AWS CLI para criar uma VPC, mais os recursos adicionais de VPC necessários para executar uma aplicação. Caso execute todos os comandos nesse procedimento, você criará uma VPC, uma sub-rede pública, uma sub-rede privada, uma tabela de rotas para cada sub-rede, um gateway da Internet, um gateway da Internet somente de saída e um gateway NAT público. Se você não precisar de todos esses recursos, poderá usar somente os comandos de exemplo necessários.

Pré-requisitos

Antes de começar, instale e configure a AWS CLI. Ao configurar a AWS CLI, você recebe uma solicitação por credenciais da AWS. Os exemplos neste procedimento pressupõem que você também tenha configurado uma região padrão. Caso contrário, adicione a opção `--region` para cada comando. Para obter informações, consulte Instalação e configuração da AWS CLI e Configuração da AWS CLI.

Tags

É possível adicionar tags a um recurso depois de criá-lo usando o comando create-tags. Como alternativa, é possível adicionar a opção `--tag-specification` ao comando de criação do recurso conforme descrito a seguir.

```
--tag-specifications ResourceType=vpc,Tags=[{Key=Name,Value=my-project}]
```

Para criar uma VPC mais recursos de VPC com a AWS CLI

1. Use o comando create-vpc a seguir para criar uma VPC com o bloco CIDR IPv4 especificado.

   ```
   aws ec2 create-vpc --cidr-block 10.0.0.0/24 --query Vpc.VpcId --output text
   ```

   Como alternativa, para criar uma VPC de pilha dupla, adicione a opção `--amazon-provided-ipv6-cidr-block` para adicionar um bloco CIDR IPv6 fornecido pela Amazon, conforme mostrado no exemplo a seguir.

   ```
   aws ec2 create-vpc --cidr-block 10.0.0.0/24 --amazon-provided-ipv6-cidr-block --
   query Vpc.VpcId --output text
   ```

   Esses comandos retornam o ID da nova VPC. Veja um exemplo a seguir.

```
vpc-1a2b3c4d5e6f1a2b3
```

2. [VPC de pilha dupla] Obtenha o bloco CIDR IPv6 associado à sua VPC usando o comando describe-vpcs a seguir.

```
aws ec2 describe-vpcs --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
 Vpcs[].Ipv6CidrBlockAssociationSet[].Ipv6CidrBlock --output text
```

O seguinte é um exemplo de saída.

```
2600:1f13:cfe:3600::/56
```

3. Crie uma ou mais sub-redes, dependendo do seu caso de uso. Em um ambiente de produção, recomendamos que você inicie recursos em ao menos duas zonas de disponibilidade. Use um dos comandos a seguir para criar cada sub-rede.

   - Sub-rede somente IPv4: para criar uma sub-rede com um bloco CIDR IPv4 específico, use o comando create-subnet a seguir.

```
aws ec2 create-subnet --vpc-id vpc-1a2b3c4d5e6f1a2b3 --cidr-block 10.0.1.0/20
 --availability-zone us-east-2a --query Subnet.SubnetId --output text
```

   - Sub-rede de pilha dupla: se você criou uma VPC de pilha dupla, é possível usar a opção `--ipv6-cidr-block` para criar uma sub-rede de pilha dupla, conforme mostrado no comando a seguir.

```
aws ec2 create-subnet --vpc-id vpc-1a2b3c4d5e6f1a2b3 --cidr-block 10.0.1.0/20
 --ipv6-cidr-block 2600:1f13:cfe:3600::/64 --availability-zone us-east-2a --
query Subnet.SubnetId --output text
```

   - Sub-rede somente IPv6: se você criou uma VPC de pilha dupla, é possível usar a opção `--ipv6-native` para criar uma sub-rede somente IPv6, conforme mostrado no comando a seguir.

```
aws ec2 create-subnet --vpc-id vpc-1a2b3c4d5e6f1a2b3 --ipv6-native --ipv6-
cidr-block 2600:1f13:cfe:3600::/64 --availability-zone us-east-2a --query
 Subnet.SubnetId --output text
```

Esses comandos retornam o ID da nova sub-rede. Veja um exemplo a seguir.

```
subnet-1a2b3c4d5e6f1a2b3
```

4. Se você precisar de uma sub-rede pública para seus servidores da Web ou para um gateway NAT, faça o seguinte:

   a. Crie um gateway da Internet usando o comando create-internet-gateway a seguir. O comando retorna o ID do novo gateway da Internet.

   ```
   aws ec2 create-internet-gateway --query InternetGateway.InternetGatewayId --
   output text
   ```

   b. Anexe o gateway da Internet à sua VPC usando o comando attach-internet-gateway a seguir. Use o ID do gateway da Internet retornado da etapa anterior.

   ```
   aws ec2 attach-internet-gateway --vpc-id vpc-1a2b3c4d5e6f1a2b3 --internet-
   gateway-id igw-id
   ```

   c. Crie uma tabela de rotas personalizada para sua sub-rede pública usando o comando create-route-table a seguir. O comando retorna o ID da nova tabela de rotas.

   ```
   aws ec2 create-route-table --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
    RouteTable.RouteTableId --output text
   ```

   d. Crie uma rota na tabela de rotas que envie todo o tráfego IPv4 para o gateway da Internet usando o comando create-route a seguir. Use o ID da tabela de rotas para a sub-rede pública.

   ```
   aws ec2 create-route --route-table-id rtb-id-public --destination-cidr-block
    0.0.0.0/0 --gateway-id igw-id
   ```

   e. Associe a tabela de rotas à sub-rede pública usando o comando associate-route-table a seguir. Use o ID da tabela de rotas para a sub-rede pública e o ID da sub-rede pública.

   ```
   aws ec2 associate-route-table --route-table-id rtb-id-public --subnet-
   id subnet-id-public-subnet
   ```

5. [IPv6] Também é possível adicionar um gateway da Internet apenas de saída para que instâncias em uma sub-rede privada possam acessar a Internet por IPv6 (por exemplo, para obter atualizações de software), mas os hosts na Internet não possam acessar suas instâncias.

a. Crie um gateway da Internet somente de saída usando o comando create-egress-only-internet-gateway a seguir. O comando retorna o ID do novo gateway da Internet.

```
aws ec2 create-egress-only-internet-gateway --vpc-id vpc-1a2b3c4d5e6f1a2b3 --
query EgressOnlyInternetGateway.EgressOnlyInternetGatewayId --output text
```

b. Crie uma tabela de rotas personalizada para sua sub-rede privada usando o comando create-route-table a seguir. O comando retorna o ID da nova tabela de rotas.

```
aws ec2 create-route-table --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
 RouteTable.RouteTableId --output text
```

c. Crie uma rota na tabela de rotas para a sub-rede privada que envie todo o tráfego IPv6 para o gateway da Internet somente de saída usando o comando create-route a seguir. Use o ID da tabela de rotas retornada na etapa anterior.

```
aws ec2 create-route --route-table-id rtb-id-private --destination-cidr-
block ::/0 --egress-only-internet-gateway eigw-id
```

d. Associe a tabela de rotas à sub-rede privada usando o comando associate-route-table a seguir.

```
aws ec2 associate-route-table --route-table-id rtb-id-private --subnet-
id subnet-id-private-subnet
```

6. Se você precisar de um gateway NAT para seus recursos em uma sub-rede privada, faça o seguinte:

a. Crie um endereço IP elástico para o gateway NAT usando o comando allocate-address a seguir.

```
aws ec2 allocate-address --domain vpc --query AllocationId --output text
```

b. Crie um gateway NAT na sub-rede pública usando o comando create-nat-gateway a seguir. Use o ID de alocação retornado da etapa anterior.

```
aws ec2 create-nat-gateway --subnet-id subnet-id-public-subnet --allocation-
id eipalloc-id
```

c. (Opcional) Se você já criou uma tabela de rotas para a sub-rede privada na etapa 5, pule essa etapa. Caso contrário, use o comando create-route-table a seguir para criar uma tabela de rotas para sua sub-rede privada. O comando retorna o ID da nova tabela de rotas.

```
aws ec2 create-route-table --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
 RouteTable.RouteTableId --output text
```

d. Crie uma rota na tabela de rotas para a sub-rede privada que envie todo o tráfego IPv4 para o gateway NAT usando o comando create-route a seguir. Use o ID da tabela de rotas para a sub-rede privada que você criou nesta etapa ou na etapa 5.

```
aws ec2 create-route --route-table-id rtb-id-private --destination-cidr-
block 0.0.0.0/0 --gateway-id nat-id
```

e. (Opcional) Se você já associou uma tabela de rotas para a sub-rede privada na etapa 5, pule essa etapa. Caso contrário, use o comando associate-route-table a seguir para associar a tabela de rotas à sub-rede privada. Use o ID da tabela de rotas para a sub-rede privada que você criou nesta etapa ou na etapa 5.

```
aws ec2 associate-route-table --route-table-id rtb-id-private --subnet-
id subnet-id-private-subnet
```

Visualizar os recursos em sua VPC

Esta seção descreve como acessar uma representação visual dos recursos em sua VPC usando a guia Mapa de recursos. Os seguintes recursos estão visíveis no mapa de recursos:

- VPC
- Sub-redes
  - A zona de disponibilidade é representada por uma letra.
  - As sub-redes públicas são verdes.
  - As sub-redes privadas são azuis.
- Tabelas de rotas
- Gateways da Internet
- Gateways da Internet apenas de saída

- Gateways NAT
- Endpoints de gateway (Amazon S3 e Amazon DynamoDB)

O mapa de recursos mostra as relações entre os recursos dentro de uma VPC e como o tráfego flui das sub-redes para os gateways NAT, o gateway da Internet e os endpoints de gateway.

Você pode usar o mapa de recursos para entender a arquitetura de uma VPC, ver quantas sub-redes ela contém, quais sub-redes estão associadas a quais tabelas de rotas e quais tabelas de rotas têm rotas para gateways NAT, gateways de Internet e endpoints de gateway.

Você também pode usar o mapa de recursos para identificar configurações indesejáveis ou incorretas, como sub-redes privadas desconectadas dos gateways NAT ou sub-redes privadas com uma rota diretamente para o gateway da Internet. Você pode escolher recursos no mapa de recursos, como tabelas de rotas, e editar as configurações desses recursos.

Para visualizar os recursos em sua VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha VPCs.
3. Selecionar a VPC.
4. Escolha a guia Mapa de recursos para exibir uma visualização dos recursos.
5. Escolha Mostrar detalhes para visualizar os detalhes, além dos IDs e zonas dos recursos exibidos por padrão.

    - VPC: os intervalos CIDR de IPv4 e IPv6 atribuídos à VPC.
    - Sub-redes: os intervalos CIDR de IPv4 e IPv6 atribuídos a cada sub-rede.
    - Tabelas de rotas: as associações de sub-rede e o número de rotas na tabela de rotas.
    - Conexões de rede: os detalhes relacionados a cada tipo de conexão:
        - Se houver sub-redes públicas na VPC, haverá um recurso de gateway da Internet com o número de rotas e as sub-redes de origem e destino para o tráfego usando o gateway da Internet.
        - Se houver um gateway da Internet somente de saída, haverá um recurso de gateway da Internet somente de saída com o número de rotas e as sub-redes de origem e destino para o tráfego usando o gateway da Internet somente de saída.
        - Se houver um gateway NAT, haverá um recurso do gateway NAT com o número de interfaces de rede e endereços IP elásticos para o gateway NAT.

- Se houver um endpoint de gateway, haverá um recurso de endpoint de gateway com o nome do serviço da AWS (Amazon S3 ou Amazon DynamoDB) ao qual você poderá se conectar usando o endpoint.

6. Passe o mouse sobre um recurso para ver a relação entre os recursos. Linhas sólidas representam relações entre recursos. As linhas pontilhadas representam o tráfego da rede para as conexões de rede.

Adicionar ou remover um bloco CIDR da sua VPC

Esta seção descreve como adicionar ou remover blocos CIDR IPv4 e IPv6 de uma VPC.

Important

- Sua VPC pode ter até cinco blocos CIDR IPv4 e cinco blocos CIDR IPv6 por padrão, mas esse limite é ajustável. Para ter mais informações, consulte Cotas da Amazon VPC. Para obter informações sobre restrições em blocos CIDR para uma VPC, consulte Blocos CIDR da VPC.
- Se a VPC tiver mais de um bloco CIDR IPv4 associado a ela, será possível remover um bloco CIDR IPv4 da VPC. Você não pode remover o bloco CIDR IPv4 principal. Você deve remover um bloco CIDR inteiro. Não é possível remover um subconjunto de um bloco CIDR ou um intervalo mesclado de blocos CIDR. Você deve primeiro excluir todas as sub-redes no bloco CIDR.
- Se não quiser mais compatibilidade com IPv6 em sua VPC, mas deseja continuar usando sua VPC para criar e se comunicar com recursos IPv4, é possível remover o bloco CIDR IPv6.
- Para remover um bloco CIDR IPv6, você deve primeiro cancelar a atribuição de quaisquer endereços IPv6 atribuídos a qualquer instância em sua sub-rede.
- Remover um bloco CIDR IPv6 não exclui automaticamente nenhuma regra do grupo de segurança, regra de ACL de rede ou rota da tabela de rotas que você configurou para redes IPv6. Você deve modificar manualmente ou excluir essas regras ou rotas.

Para adicionar ou remover um bloco CIDR de uma VPC usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.

2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Selecione a VPC e escolha Actions (Ações), Edit CIDRs (Editar CIDRs).
4. Para remover um CIDR, escolha Remover ao lado do CIDR.
5. Para adicionar um CIDR, escolha Adicionar novo CIDR IPv4 ou Adicionar novo CIDR IPv6.
6. Para adicionar um CIDR para Bloco CIDR IPv4, execute uma das seguintes ações:
   - Escolha IPv4 CIDR manual input (Entrada manual de CIDR IPv4) e insira um bloco CIDR IPv4.
   - Escolha IPAM-allocated IPv4 CIDR (CIDR IPv4 alocado por IPAM) e selecione um CIDR de um grupo IPAM IPv4.
   - Escolha Salvar.
7. Para adicionar um CIDR para Bloco CIDR IPv6, faça o seguinte:

   - Escolha o bloco CIDR IPv6 alocado pelo IPAM se estiver usando o Amazon VPC IP Address Manager e quiser provisionar um CIDR IPv6 de um grupo do IPAM. Você tem duas opções para provisionar um intervalo de endereços de IP para a VPC no bloco CIDR:
     - Comprimento da máscara de rede: Escolha essa opção para selecionar um comprimento de máscara de rede para o CIDR. Execute um destes procedimentos:
       - Se um comprimento de máscara de rede padrão estiver previamente escolhido para o grupo do IPAM, é possível optar por Padrão" para o comprimento de máscara de rede do IPAM e utilizar o comprimento padrão estabelecido para o grupo do IPAM pelo administrador do IPAM. Para informações detalhadas sobre a regra opcional de alocação de comprimento de máscara de rede padrão, consulte o Guia do usuário do IPAM do Amazon VPC na seção sobre a criação de um grupo de IPv6 regional.
       - Caso não haja um comprimento de máscara de rede padrão definido para o grupo do IPAM, é necessário selecionar um comprimento de máscara de rede que seja mais específico que o comprimento da máscara de rede do CIDR associado ao grupo do IPAM. Por exemplo, se o CIDR do grupo do IPAM for /50, você poderá escolher um comprimento de máscara de rede entre /52 e /60 para a VPC. Os comprimentos possíveis da máscara de rede estão entre /44 e /60 em incrementos de /4.
     - Selecione um CIDR: escolha essa opção para inserir manualmente um endereço IPv6. Você só pode escolher um comprimento de máscara de rede que seja mais específico do que o comprimento da máscara de rede do CIDR do grupo do IPAM. Por exemplo, se o CIDR do grupo do IPAM for /50, você poderá escolher um comprimento de máscara de rede entre /52

e /60 para a VPC. Os possíveis comprimentos de máscara de rede IPv6 estão entre /44 e /60 em incrementos de /4.

- Escolha Bloco CIDR IPv6 fornecido pela Amazon para solicitar um bloco CIDR IPv6 do grupo de endereços IPv6 da Amazon. Em Network Border Group (Grupo de borda de rede), selecione o grupo do qual a AWS anuncia endereços IP. A Amazon fornece um tamanho de bloco CIDR IPv6 fixo de /56.
- Escolha CIDR IPv6 de minha propriedade para provisionar um CIDR IPv6 que você já trouxe para o AWS. Para obter mais informações sobre como trazer seus próprios intervalos de endereços de IP para a AWS, consulte Traga seus próprios endereços IP (BYOIP) para o Amazon EC2 no Guia do usuário do Amazon EC2. Você tem duas opções para provisionar um intervalo de endereços de IP para a VPC no bloco CIDR:
  - Sem preferência: Escolha essa opção para usar o comprimento da máscara de rede de /56.
  - Selecionar um CIDR: escolha essa opção para inserir manualmente um endereço IPv6 e escolher um comprimento de máscara de rede que seja mais específico do que o tamanho do CIDR do BYOIP. Por exemplo, se o CIDR do grupo BYOIP for /50, você poderá escolher um comprimento de máscara de rede entre /52 e /60 para o VPC. Os possíveis comprimentos de máscara de rede IPv6 estão entre /44 e /60 em incrementos de /4.
  - Escolha Selecionar CIDR quando terminar.

8. Escolha Fechar.
9. Se você adicionou um bloco CIDR a sua VPC, é possível criar sub-redes que usam o novo bloco CIDR. Para ter mais informações, consulte Criar uma sub-rede.

Para associar ou desassociar um bloco CIDR de uma VPC usando a AWS CLI

Use os comandos associate-vpc-cidr-block e disassociate-vpc-cidr-block.

Conjuntos de opções DHCP no Amazon VPC

Dispositivos de rede na VPC usam o Protocolo de Configuração Dinâmica de Host (DHCP). Você pode usar conjuntos de opções DHCP para controlar os seguintes aspectos da configuração de rede na sua rede virtual:

- Os servidores DNS, nomes de domínio ou servidores NTP (Network Time Protocol) usados pelos dispositivos na sua VPC.
- Se a resolução de DNS está habilitada ou não na VPC.

Conteúdo

O que é DHCP?

Todo dispositivo em uma rede TCP/IP requer um endereço IP para se comunicar pela rede. No passado, os endereços IP tinham que ser atribuídos manualmente a cada dispositivo na rede. Hoje, os endereços IP são atribuídos dinamicamente por servidores de Protocolo de Configuração Dinâmica de Host (DHCP).

As aplicações executadas em instâncias do EC2 podem se comunicar com servidores DHCP da Amazon conforme necessário para recuperar a concessão de endereço IP ou outras informações de configuração de rede (como o endereço IP de um servidor DNS da Amazon ou o endereço IP do roteador da VPC).

Você pode especificar as configurações de rede fornecidas pelos servidores DHCP da Amazon usando conjuntos de opções DHCP.

Se você tiver uma configuração de VPC que exija que suas aplicações façam solicitações diretas ao servidor DHCP IPv6 da Amazon, observe o seguinte:

- Uma instância do EC2 em uma sub-rede de pilha dupla só pode recuperar seu endereço IPv6 do servidor DHCP IPv6. Ela não pode recuperar nenhuma configuração de rede adicional do servidor DHCP IPv6, como nomes de servidor DNS ou nomes de domínio.
- Uma instância do EC2 em uma sub-rede somente IPv6 pode recuperar seu endereço IPv6 do servidor DHCP IPv6 e pode recuperar informações adicionais de configuração de rede, como nomes de servidor DNS e nomes de domínio.
- Para uma instância do EC2 em uma sub-rede somente IPv6, o servidor DHCP IPv4 retornará 169.254.169.253 como o servidor de nomes se “AmazonProvidedDNS” for explicitamente mencionado no conjunto de opções de DHCP. Se “AmazonProvideDDNS” estiver ausente do conjunto de opções, o servidor DHCP IPv4 não retornará um endereço, independentemente de outros servidores de nomes IPv4 serem mencionados no conjunto de opções ou não.

Os servidores DHCP da Amazon também podem fornecer um prefixo IPv4 ou IPv6 inteiro para uma interface de rede na sua VPC usando delegação de prefixo (consulte Atribuir prefixos a interfaces

de rede do Amazon EC2 no Guia do usuário do Amazon EC2). A delegação de prefixo IPv4 não é fornecida em respostas DHCP. É possível usar o IMDS para recuperar prefixos IPv4 atribuídos à interface (consulte Categorias de metadados da instância no Guia do usuário do Amazon EC2).

Conceitos do conjunto de opções DHCP

Um conjunto de opções DHCP é um grupo de configurações de rede usado pelos recursos na sua VPC, como instâncias do EC2, para se comunicar pela sua rede virtual.

Cada região tem um conjunto de opções DHCP padrão. Cada VPC usa o conjunto de opções DHCP padrão de sua região, a menos que você crie e associe um conjunto de opções DHCP personalizado à VPC ou configure-a sem um conjunto de opções DHCP.

Se sua VPC não tiver um conjunto de opções de DHCP configurado:

- Para as instâncias do EC2 criadas no Nitro System, a AWS configurará `169.254.169.253` como o servidor de nomes de domínio padrão.
- Para as instâncias do EC2 criadas no Xen, nenhum servidor de nomes de domínio será configurado e, como as instâncias na VPC não terão acesso a um servidor de DNS, elas não poderão acessar a Internet.

Você pode associar um conjunto de opções DHCP a várias VPCs, mas cada VPC pode ter somente um conjunto de opções DHCP associado.

Se você excluir uma VPC, o conjunto de opções DHCP associado à VPC será desassociado dela.

Conteúdo

Conjunto padrão de opções de DHCP

O conjunto de opções DHCP padrão contém as seguintes configurações:

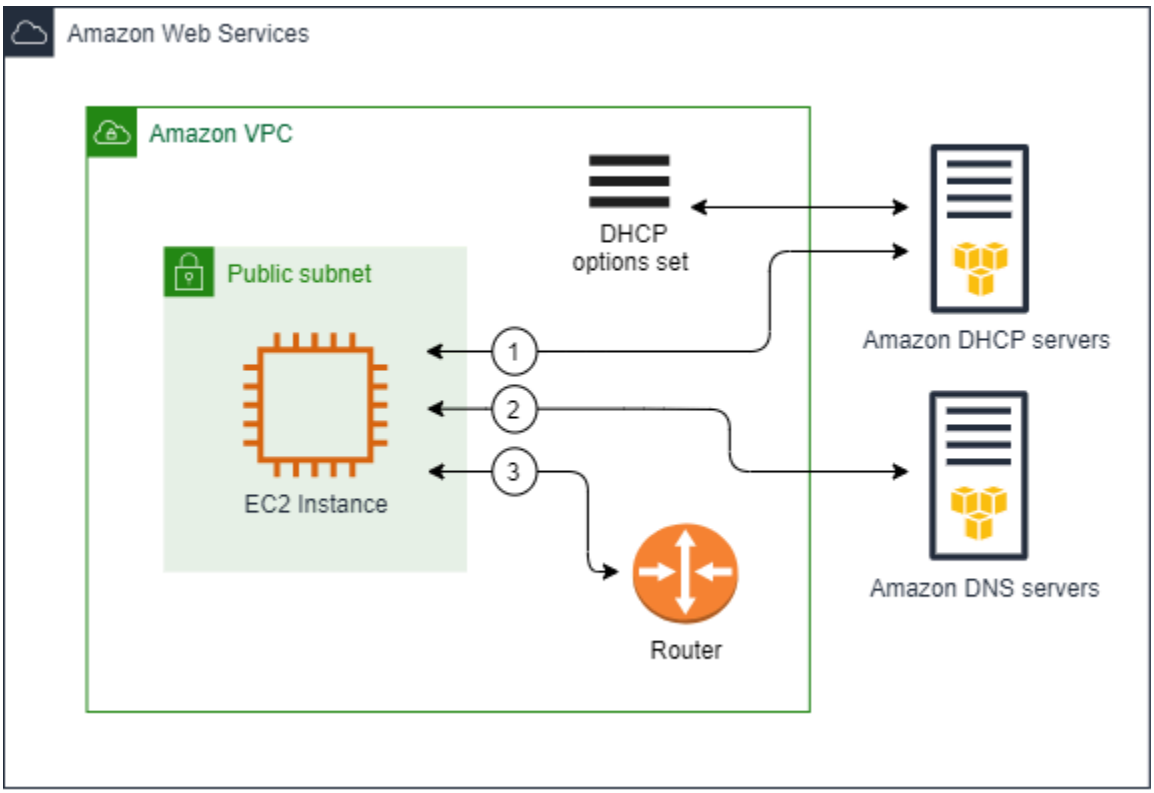
- Servidores de nomes DNS: os servidores de nomes DNS que as interfaces de rede usam para resolução de nomes de domínio. Para um conjunto de opções DHCP padrão, isso é sempre `AmazonProvidedDNS`. Para ter mais informações, consulte Servidor de DNS da Amazon.

- Nome de domínio: o nome de domínio que um cliente deve usar ao resolver nomes de host usando o Sistema de Nomes de Domínio (DNS). Para obter mais informações sobre os nomes de domínios usados para instâncias do EC2, consulte Nomes de host de instâncias do Amazon EC2.
- Tempo de locação preferencial de IPv6: a frequência com que uma instância em execução com um IPv6 atribuído a ela passa pela renovação do leasing DHCPv6. O tempo de locação padrão é 140 segundos. A renovação da locação geralmente ocorre quando a metade do tempo da locação já passou.

Quando você usa um conjunto de opções DHCP padrão, as seguintes configurações não são usadas, mas existem padrões para instâncias do EC2:

- Servidores NTP: por padrão, as instâncias do EC2 usam o Serviço de Sincronização Temporal da Amazon para obter a hora.
- Servidores de nomes NetBIOS: para instâncias do EC2 que executam o Windows, o nome NetBIOS do computador é um nome amigável atribuído à instância para identificá-la na rede. O servidor de nomes NetBIOS mantém uma lista de mapeamentos entre nomes NetBIOS de computadores e endereços de rede para redes que usam o NetBIOS como seu serviço de nomenclatura.
- Tipo de nó NetBIOS: para instâncias do EC2 que executam o Windows, é o método que as instâncias usam para resolver nomes NetBIOS para endereços IP.

Quando você usa o conjunto de opções padrão, o servidor DHCP da Amazon usa as configurações de rede no conjunto de opções padrão. Quando você executa instâncias na sua VPC, elas fazem o seguinte, conforme mostrado no diagrama: (1) interagem com o servidor DHCP, (2) interagem com o servidor DNS da Amazon e (3) conectam-se a outros dispositivos na rede por meio do roteador para sua VPC. As instâncias podem interagir com o servidor DHCP da Amazon a qualquer momento para obter a concessão de endereço IP e as configurações adicionais da rede.



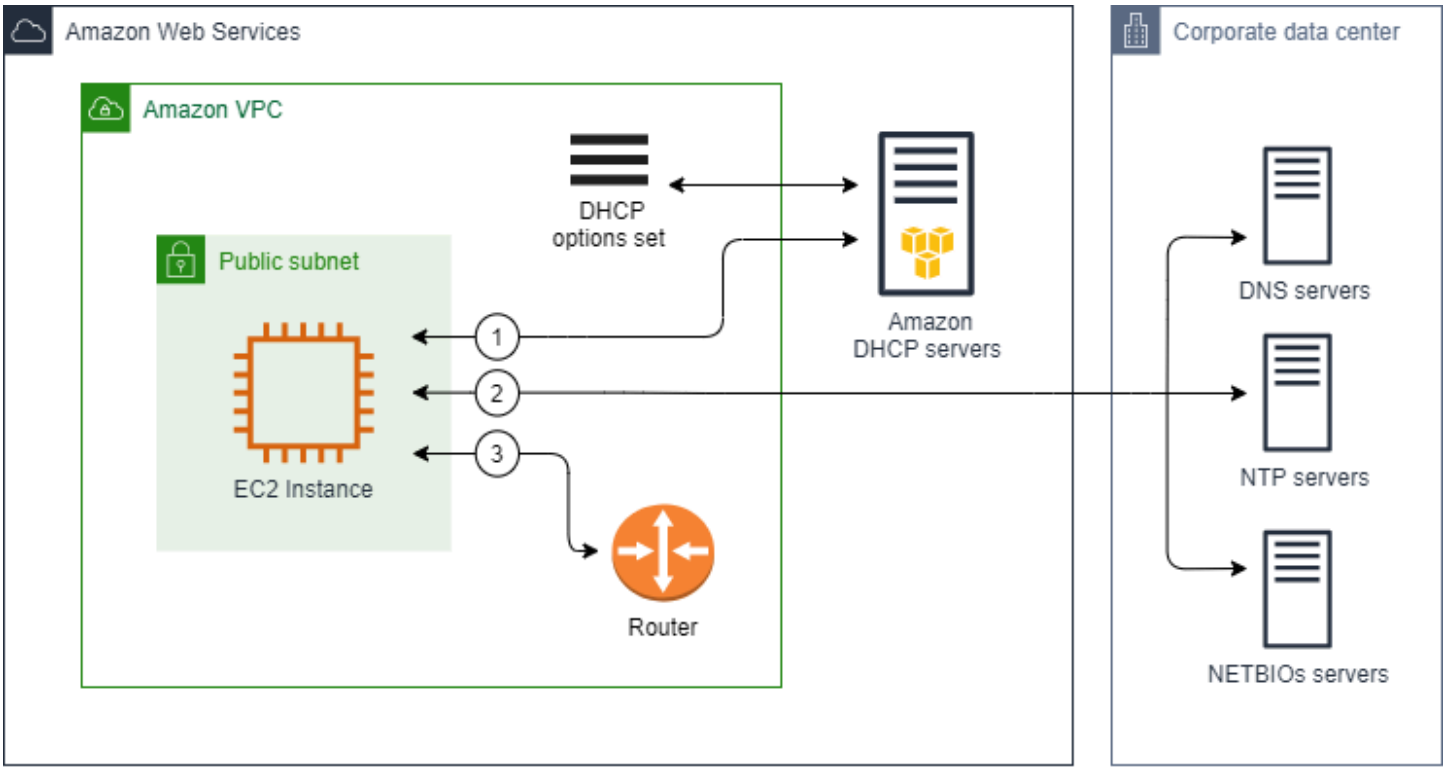
Conjunto personalizado de opções de DHCP

É possível criar um conjunto de opções DHCP personalizado com as seguintes configurações e, em seguida, associá-lo a uma VPC:

- Servidores de nomes DNS: os servidores de nomes DNS que as interfaces de rede usam para resolução de nomes de domínio.
- Nome de domínio: o nome de domínio que um cliente usa ao resolver nomes de host usando o Sistema de Nomes de Domínio (DNS).
- Servidores NTP: os servidores NTP que fornecem a hora para as instâncias.
- Servidores de nomes NetBIOS: para instâncias do EC2 que executam o Windows, o nome NetBIOS do computador é um nome amigável atribuído à instância para identificá-la na rede. Um servidor de nomes NetBIOS mantém uma lista de mapeamentos entre nomes NetBIOS de computadores e endereços de rede para redes que usam o NetBIOS como seu serviço de nomenclatura.
- Tipo de nó NetBIOS: para instâncias do EC2 que executam o Windows, esse é o método que as instâncias usam para resolver nomes NetBIOS para endereços IP.
- Tempo de locação preferencial de IPv6 (opcional): um valor (em segundos, minutos, horas ou anos) da frequência com que uma instância em execução com um IPv6 atribuído a ela passa pela

renovação do leasing de DHCPv6. Os valores aceitáveis estão entre 140 e 4294967295 segundos (aproximadamente 138 anos). Se nenhum valor for fornecido, o tempo de locação padrão será 140 segundos. Se você usar endereçamento de longo prazo para instâncias do EC2, poderá aumentar o tempo de locação e evitar solicitações frequentes de renovação de leasing. A renovação da locação geralmente ocorre quando a metade do tempo da locação já passou.

Quando você usa um conjunto de opções personalizado, as instâncias iniciadas na sua VPC fazem o seguinte, conforme mostrado no diagrama: (1) usam as configurações de rede no conjunto de opções DHCP personalizado, (2) interagem com os servidores DNS, NTP e NetBIOS especificados no conjunto de opções DHCP personalizado e (3) conectam-se a outros dispositivos na rede por meio do roteador para sua VPC.



Tarefas relacionadas

- Criar um conjunto de opções DHCP
- Alterar o conjunto de opções associado a uma VPC

Trabalhar com conjuntos de opções DHCP

Use os procedimentos a seguir para visualizar e trabalhar com conjuntos de opções DHCP. Para obter mais informações sobre como funcionam os conjuntos de opções DHCP, consulte the section called “Conceitos do conjunto de opções DHCP”:

Tarefas

- Criar um conjunto de opções DHCP
- Alterar o conjunto de opções associado a uma VPC
- Excluir um conjunto de opções DHCP

Criar um conjunto de opções DHCP

Um conjunto de opções DHCP personalizado permite que você personalize a VPC com seu próprio servidor DNS, nome de domínio etc. Você pode criar tantos conjuntos adicionais de opções DHCP quantos desejar. No entanto, você só pode associar uma VPC a um conjunto de opções DHCP de cada vez.

> **Note**
>
> Após criar um conjunto de opções DHCP, você não pode modificá-lo. Para atualizar as opções DHCP da sua VPC, você deve criar um novo conjunto de opções DHCP e associá-lo a ela.

Para criar um conjunto de opções DHCP usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha DHCP Option Sets (Conjuntos de opções DHCP).
3. Escolha Create DHCP Options set.
4. Para Tag settings, (Configurações de etiqueta), opcionalmente, insira um nome para o conjunto de opções DHCP. Se você inserir um valor, ele criará automaticamente um nome de etiqueta para o conjunto de opções DHCP.
5. Para Opções DHCP, forneça as configurações necessárias.

    - Domain name (Nome de domínio) (opcional): insira o nome de domínio que um cliente deve usar ao resolver nomes de host pelo Sistema de Nomes de Domínio. Se você não estiver

usando o AmazonProvidedDNS, seus servidores de nomes de domínio personalizados deverão determinar o nome do host, conforme apropriado. Se você usar uma zona hospedada privada do Amazon Route 53, poderá usar AmazonProvideDNS. Para ter mais informações, consulte Atributos de DNS para sua VPC.

> **Note**
>
> Use somente nomes de domínio que você tenha total controle.

Alguns sistemas operacionais Linux aceitam vários nomes de domínio separados por espaços. No entanto, outros sistemas operacionais Windows e Linux tratam o valor como um domínio único, o que resulta em um comportamento inesperado. Se o seu conjunto de opções DHCP estiver associado a uma VPC que contenha instâncias que executam sistemas operacionais que tratam o valor como um domínio único, especifique somente um nome de domínio.

- Domain name servers (Servidores de nomes de domínio) (opcional): insira os servidores DNS que serão usados para resolver o endereço IP de um host com base no nome do host.

  Você pode inserir **`AmazonProvidedDNS`** ou servidores de nomes de domínio personalizados. Usar ambos pode causar comportamento inesperado. Você pode inserir endereços IP de até quatro servidores de nomes de domínio IPv4 (ou até três servidores de nomes de domínio IPv4 e **`AmazonProvidedDNS`**) e quatro servidores de nomes de domínio IPv6 separados por vírgulas. Embora você possa especificar até oito servidores de nomes de domínio, alguns sistemas operacionais podem impor limites inferiores. Para obter mais informações sobre o AmazonProvidedDNS e o servidor do Amazon DNS, consulte Servidor de DNS da Amazon.

  > **Important**
  >
  > Se a VPC tiver um gateway da Internet, certifique-se de especificar seu próprio servidor DNS ou um servidor DNS da Amazon (AmazonProvidedDNS) para o valor Servidores de nomes de domínio. Caso contrário, as instâncias na VPC não terão acesso ao DNS, o que desabilita o acesso à Internet.

- NTP servers (Servidores NTP) (opcional): Insira os endereços IP de até oito servidores Network Time Protocol (NTP) (quatro endereços IPv4 e quatro endereços IPv6).

Os servidores NTP fornecem as horas para a rede. Você pode especificar o Amazon Time Sync Service no endereço IPv4 `169.254.169.123` ou endereço IPv6 `fd00:ec2::123`. As instâncias se comunicam com o Amazon Time Sync Service por padrão. O endereço IPv6 só pode ser acessado nas instâncias do EC2 criadas no Nitro System.

Para mais informações sobre a opção de servidores NTP, consulte o RFC 2132. Para mais informações sobre o Serviço de Sincronização Temporal da Amazon, consulte Definir a hora da instância no Guia do usuário do Amazon EC2.

- NetBIOS name servers (Servidores de nomes NetBIOS) (opcional): insira os endereços IP de até quatro servidores de nomes NetBIOS.

  Para instâncias do EC2 que executam o Windows, o nome NetBIOS do computador é um nome amigável atribuído à instância para identificá-la na rede. O servidor de nomes NetBIOS mantém uma lista de mapeamentos entre nomes NetBIOS de computadores e endereços de rede para redes que usam o NetBIOS como seu serviço de nomenclatura.

- NetBIOS node type (Tipo de nó NetBIOS) (opcional): insira **1**, **2**, **4** ou **8**. Recomendamos que você especifique **2** (ponto a ponto ou nó P). A transmissão e o multicast não são compatíveis no momento. Para obter mais informações sobre esses tipos de nó, consulte a seção 8.7 do RFC 2132 e a seção 10 do RFC 1001.

  Para instâncias do EC2 que executam o sistema operacional Windows, esse é o método que as instâncias usam para resolver nomes NetBIOS para endereços IP. No conjunto padrão de opções, não há um valor para o tipo de nó NetBIOS.

- Tempo de locação preferencial de IPv6 (opcional): um valor (em segundos, minutos, horas ou anos) da frequência com que uma instância em execução com um IPv6 atribuído a ela passa pela renovação do leasing de DHCPv6. Os valores aceitáveis estão entre 140 e 2147483647 segundos (aproximadamente 68 anos). Se nenhum valor for fornecido, o tempo de locação padrão será 140 segundos. Se você usar endereçamento de longo prazo para instâncias do EC2, poderá aumentar o tempo de locação e evitar solicitações frequentes de renovação de leasing. A renovação da locação geralmente ocorre quando a metade do tempo da locação já passou.

6. Adicione Tags (Etiquetas).
7. Escolha Create DHCP Options set. Anote o nome ou ID do novo conjunto de opções DHCP.
8. Para configurar a VPC para usar o novo conjunto de opções, consulte Alterar o conjunto de opções associado a uma VPC.

Para criar um conjunto de opções DHCP para sua VPC usando a linha de comando

- create-dhcp-options (AWS CLI)
- New-EC2DhcpOption (AWS Tools for Windows PowerShell)

Alterar o conjunto de opções associado a uma VPC

Depois de criar um conjunto de opções DHCP, você pode associá-lo a uma ou mais VPCs. É possível associar somente um conjunto de opções DHCP a uma VPC de cada vez. Se você não associar um conjunto de opções DHCP a uma VPC, desabilitará a resolução de nomes de domínio na VPC.

Depois de associar um novo conjunto de opções DHCP a uma VPC, todas as instâncias existentes e todas as novas instâncias iniciadas nessa VPC usarão as novas opções. Não é necessário reiniciar ou executar novamente suas instâncias. As instâncias recuperam automaticamente as mudanças dentro de algumas horas, dependendo da frequência com que renovam suas concessões DHCP. Se você preferir, é possível renovar explicitamente a concessão usando o sistema operacional na instância.

Para alterar o conjunto de opções DHCP associado a uma VPC usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Marque a caixa de seleção da VPC e escolha Actions (Ações), Edit VPC Settings (Editar configurações de VPC).
4. Para DHCP options set (Conjunto de opções DHCP), escolha o conjunto de opções DHCP. Como alternativa, escolha Nenhum conjunto de opções DHCP para desabilitar a resolução de nomes de domínio para a VPC.
5. Escolha Salvar.

Para alterar o conjunto de opções DHCP associado a uma VPC usando a linha de comando

- associate-dhcp-options (AWS CLI)
- Register-EC2DhcpOption (AWS Tools for Windows PowerShell)

Excluir um conjunto de opções DHCP

Quando você não precisar mais de um conjunto de opções de DHCP, use o procedimento a seguir para excluí-lo. Não é possível excluir um conjunto de opções DHCP quando ele está em uso. Para cada VPC associada ao conjunto de opções DHCP a ser excluído, você deve associar um conjunto de opções DHCP diferente à VPC ou configurá-la para não usar um conjunto de opções DHCP. Para ter mais informações, consulte the section called “Alterar o conjunto de opções associado a uma VPC”.

Para excluir um conjunto de opções DHCP usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha DHCP Option Sets (Conjuntos de opções DHCP).
3. Selecione o botão de opção para o conjunto de opções DHCP e escolha Ações, Excluir conjunto de opções DHCP.
4. Quando for instruído a confirmar, digite **`delete`** e escolha Excluir conjunto de opções DHCP.

Para excluir um conjunto de opções DHCP usando a linha de comando

- delete-dhcp-options (AWS CLI)
- Remove-EC2DhcpOption (AWS Tools for Windows PowerShell)

Atributos de DNS para sua VPC

Domain Name System (DNS) é um padrão por meio do qual os nomes usados na Internet são determinados de acordo com os endereços IP correspondentes. O nome de host DNS é aquele que é atribuído exclusiva e absolutamente a um computador; ele é formado por um nome de host e um nome de domínio. Os servidores DNS determinam os nomes do host DNS de acordo com os endereços IP correspondentes.

Os endereços IPv4 públicos habilitam a comunicação pela Internet e os endereços IPv4 privados habilitam a comunicação na rede da instância. Para ter mais informações, consulte Endereçamento IP para suas VPCs e sub-redes.

A Amazon fornece um servidor DNS (o Amazon Route 53 Resolver) à VPC. Para usar seu próprio servidor DNS, crie um novo conjunto de opções de DHCP para a VPC. Para ter mais informações, consulte Conjuntos de opções DHCP no Amazon VPC.

Conteúdo

Noções básicas sobre o Amazon DNS

Como arquiteto ou administrador da AWS, um dos componentes de rede fundamentais que você encontrará é o servidor Amazon DNS, também conhecido como Route 53 Resolver. Esse serviço de resolução de DNS é nativamente integrado a cada zona de disponibilidade em sua região da AWS, fornecendo uma solução confiável e escalável para resolução de nomes de domínio em sua nuvem privada virtual (VPC). Nesta seção, você aprenderá sobre os endereços IP do servidor Amazon DNS, os nomes de host DNS privados que ele pode resolver e as regras que governam seu uso.

Conteúdo

Servidor de DNS da Amazon

O Route 53 Resolver (também chamado de “servidor Amazon DNS” ou “AmazonProvidedDNS”) é um serviço de resolução de DNS incorporado em cada zona de disponibilidade em uma região da AWS. O Route 53 Resolver está localizado em `169.254.169.253` (IPv4), `fd00:ec2::253` (IPv6) e no intervalo CIDR IPV4 privado primário provisionado para sua VPC mais dois. Por exemplo, se você tiver uma VPC com um CIDR IPv4 de `10.0.0.0/16` e um CIDR IPv6 de `2001:db8::/32`, é possível acessar o Route 53 Resolver em `169.254.169.253` (IPv4), `fd00:ec2::253` (IPv6) ou `10.0.0.2` (IPv4). Os recursos em uma VPC usam um endereço local de link para consultas de DNS. Essas consultas são transportadas para o Route 53 Resolver de forma privada e não são visíveis na rede. Em uma sub-rede somente IPv6, o endereço local do link IPv4 (169.254.169.253) ainda pode ser acessado, desde que "AmazonProvideDDNS" seja o servidor de nomes no conjunto de opções de DHCP.

Quando você inicia uma instância em uma VPC, fornecemos à instância um nome de host DNS privado. Também fornecemos um nome de host DNS público se a instância estiver configurada com um endereço público IPv4 e os atributos DNS da VPC estiverem habilitados.

O formato do nome do host DNS privado depende de como você configura a instância do EC2 ao iniciá-la. Para obter mais informações sobre os tipos de nomes de host DNS privados, consulte Tipos de nome de host de instância do Amazon EC2 no Guia do usuário do Amazon EC2.

O servidor de DNS da Amazon na VPC é usado para determinar os nomes de domínio DNS que você especifica em uma zona hospedada privada no Route 53. Para obter mais informações sobre zonas hospedadas privadas, consulte Trabalhar com zonas hospedadas privadas no Guia do desenvolvedor do Amazon Route 53.

Regras e considerações

Ao usar o servidor de DNS da Amazon, as seguintes regras e considerações se aplicam.

- Não é possível filtrar o tráfego de ou para um servidor de DNS da Amazon usando network ACLs ou grupos de segurança.
- Os serviços que utilizam o framework do Hadoop , como o Amazon EMR, requerem instâncias para determinar seus próprios nomes de domínio totalmente qualificados (FQDN). Nesses casos, a resolução do DNS pode falhar se a opção `domain-name-servers` estiver configurada para um valor personalizado. Para garantir uma resolução de DNS adequada, considere adicionar um encaminhador condicional no seu servidor de DNS para encaminhar consultas para o domínio *`region-name`*`.compute.internal` para o servidor de DNS da Amazon. Para obter mais informações, consulte Configurar uma VPC para hospedar clusters no Guia de gerenciamento do Amazon EMR.
- O Amazon Route 53 Resolver é compatível apenas com consultas de DNS recursivas.

Nomes de host DNS para instâncias do EC2

Quando você inicia uma instância, ela sempre recebe um endereço IPv4 privado e um nome de host DNS privado que corresponde ao seu endereço IPv4 privado. Se a instância tiver um endereço IPv4 público, os atributos DNS para a VPC determinarão se ela receberá um nome de host DNS público que corresponda ao endereço IPv4 público. Para ter mais informações, consulte Atributos de DNS para sua VPC.

Com o servidor de DNS fornecido pela Amazon habilitado, os nomes de host DNS são resolvidos conforme descrito a seguir.

Nome DNS IPv4 privado

O nome de host DNS IPv4 privado de uma instância é resolvido em seu endereço IPv4 privado. Você pode usar o nome de host DNS IPv4 privado para comunicações entre instâncias na mesma VPC ou em VPCs conectadas. Para obter mais informações, consulte Endereços IPv4 privados no Guia do usuário do Amazon EC2.

Nome DNS IPv4 público

O nome de host DNS IPv4 público de uma instância é resolvido em seu endereço IPv4 público (fora da rede da instância) ou seu endereço IPv4 privado (dentro da rede da instância). Para obter mais informações, consulte Endereços IPv4 públicos no Guia do usuário do Amazon EC2.

Para resolver nomes DNS IPv4 públicos em endereços IPv4 privados em uma conexão de emparelhamento da VPC, é necessário habilitar a resolução de DNS para a conexão de emparelhamento. Para obter mais informações, consulte Habilitar a resolução de DNS para a conexão de emparelhamento da VPC.

Nome DNS de recurso privado

O nome DNS baseado em RBN que pode determinar os registros DNS A e AAAA selecionados para esta instância. Esse nome do host DNS fica visível nos detalhes da instância para instâncias em sub-redes de pilha dual e somente IPv6. Para obter mais informações sobre o RBN, consulte Tipos de nomes do host de instâncias do EC2 no Guia do usuário do Amazon EC2.

Atributos de DNS para sua VPC

Os atributos da VPC a seguir determinam o suporte a DNS fornecido para a VPC. Se ambos os atributos estiverem habilitados, uma instância iniciada na VPC receberá um nome de host DNS público se tiver recebido um endereço IPv4 público ou um endereço IP elástico na criação. Se você ativar ambos os atributos para uma VPC que anteriormente não tinha os dois atributos, as instâncias que já tiverem sido executadas nessa VPC receberão nomes de host DNS públicos se tiverem um endereço IPv4 público ou um endereço IP elástico.

Para verificar se esses atributos estão habilitados para a VPC, consulte Exibir e atualizar atributos DNS para sua VPC.

Atributo	Descrição
`enableDnsHostnames`	Determina se a VPC oferece suporte à atribuição de nomes de host DNS públicos a instâncias com endereços IP públicos.

Atributo	Descrição
	O padrão desse atributo é `false`, a não ser que a VPC seja uma VPC padrão. Observe abaixo as Regras e considerações para esse atributo.
`enableDnsSupport`	Determina se a VPC oferece suporte à resolução de DNS por meio do servidor de DNS fornecido pela Amazon. Se esse atributo for `true`, as consultas ao servidor de DNS fornecido pela Amazon terão êxito. Para ter mais informações, consulte Servidor de DNS da Amazon. O padrão desse atributo é `true`. Observe abaixo as Regras e considerações para esse atributo.

Regras e considerações

- Se ambos os atributos estiverem definidos como `true`, ocorrerá o seguinte:
  - Instâncias com endereços IP públicos recebem nomes de host DNS públicos correspondentes.
  - O servidor Amazon Route 53 Resolver poderá determinar nomes de host DNS privados fornecidos pela Amazon.
- Se pelo menos um dos atributos estiver definido como `false`, ocorrerá o seguinte:
  - Instâncias com endereços IP públicos não recebem nomes de host DNS públicos correspondentes.
  - O Amazon Route 53 Resolver não poderá determinar nomes de host DNS privados fornecidos pela Amazon.
  - As instâncias receberão nomes de host DNS privados personalizados se houver um nome de domínio personalizado no conjunto de opções DHCP. Se você não estiver usando o servidor Amazon Route 53 Resolver, seus servidores de nomes de domínio personalizados deverão determinar o nome de host do modo apropriado.
- Se você usa nomes de domínio DNS definidos em uma zona hospedada privada no Amazon Route 53 ou usa DNS privado com endpoints da VPC de interface (AWS PrivateLink), é necessário definir os atributos `enableDnsHostnames` e `enableDnsSupport` como `true`.
- O Amazon Route 53 Resolver pode determinar nomes de host DNS privados para endereços IPv4 privados para todos os espaços de endereço, inclusive quando o intervalo de endereços IPv4

de sua VPC não se encaixar nos intervalos de endereços IPv4 privados especificados pela RFC 1918. No entanto, se você criou a VPC antes de outubro de 2016, o Amazon Route 53 Resolver não resolverá nomes de host DNS privados se o intervalo de endereços IPv4 da VPC estiver fora desses intervalos. Para habilitar o suporte para isso, entre em contato com o Support.

Cotas de DNS

Há um limite de 1.024 pacotes por segundo (PPS) para serviços que usam endereços locais do link. Esse limite inclui o agregado de consultas ao DNS do Route 53 Resolver, solicitações do Serviço de metadados de instância (IMDS), solicitações do Amazon Time Service Network Time Protocol (NTP) e solicitações do Windows Licensing Service (para instâncias baseadas no Microsoft Windows). Essa cota não pode ser aumentada.

O número de consultas de DNS por segundo com suporte do Amazon Route 53 varia, dependendo do tipo da consulta, do tamanho da resposta e do protocolo em uso. Para obter mais informações e recomendações para uma arquitetura de DNS escalável, consulte o Guia técnico DNS híbrido da AWS com Diretório Ativo.

Se você atingir a cota, o Route 53 Resolver rejeitará o tráfego. Uma das causas para a cota ser atingida pode ser um problema de controle de utilização de DNS ou consultas de metadados de instância que usam a interface de rede do Route 53 Resolver. Para obter informações sobre como resolver problemas de limitação de DNS da VPC, consulte Como posso determinar se minhas consultas de DNS ao servidor de DNS fornecido pela Amazon falham devido à limitação de DNS da VPC?. Para obter mais informações sobre a recuperação de metadados de instância, consulte Recuperar metadados de instância no Guia do usuário do Amazon EC2.

Zonas hospedadas privadas

Para acessar os recursos em seu VPC usando nomes de domínio DNS personalizados, como `example.com`, em vez de usar endereços IPv4 privados ou nomes de host DNS privados fornecidos pela AWS, você pode criar uma zona hospedada privada no Route 53. Uma zona hospedada privada é um contêiner que contém informações sobre como você deseja rotear o tráfego para um domínio e seus subdomínios dentro de uma ou mais VPCs sem expor seus recursos à Internet. Desse modo, é possível criar conjuntos de registros de recursos no Route 53, que determinam como o Route 53 responderá a consultas para o domínio e os subdomínios. Por exemplo, se desejar que as solicitações de navegador para exemplo.com sejam roteadas para um servidor web em sua VPC, você criará um registro A em sua zona hospedada privada e especificará o endereço IP desse

servidor web. Para obter mais informações sobre como criar uma zona hospedada privada, consulte Trabalhar com zonas hospedadas privadas no Guia do desenvolvedor do Amazon Route 53.

Para acessar recursos usando nomes de domínio de DNS personalizados, você deve estar conectado a uma instância dentro da VPC. Em sua instância, você pode testar se seu recurso na zona hospedada privada pode ser acessado pelo respectivo nome de DNS personalizado usando o comando `ping`; por exemplo, `ping mywebserver.example.com`. (É essencial que as regras de security group de sua instância permitam tráfego ICMP de entrada para que o comando `ping` funcione.)

Zonas hospedadas privadas não comportarão relações temporárias fora da VPC. Por exemplo, você não pode acessar seus recursos usando nomes de DNS privados do outro lado de uma conexão VPN.

> **Important**
>
> Se você usar nomes de domínio DNS personalizados definidos em uma zona hospedada privada no Amazon Route 53, deverá definir ambos os atributos `enableDnsHostnames` e `enableDnsSupport` como `true`.

Visualizar nomes de host DNS para a instância do EC2

É possível visualizar os nomes de host DNS para uma instância em execução ou uma interface de rede usando o console do Amazon EC2 ou a linha de comando. Conhecer esses nomes de host é importante para se conectar aos seus recursos.

Os campos Public DNS (IPv4) (DNS público (IPv4)) e Private DNS (DNS privado) ficam disponíveis quando as opções de DNS estão ativadas para a VPC associada à instância. Para ter mais informações, consulte the section called “Atributos de DNS para sua VPC”.

Instância

Para visualizar nomes de host DNS para uma instância por meio do console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione sua instância na lista.

4. No painel de detalhes, os campos Public DNS (IPv4) e Private DNS exibem os nomes de host DNS, se aplicável.

Para visualizar nomes de host DNS para uma instância por meio da linha de comando

- describe-instances (AWS CLI)
- Get-EC2Instance (AWS Tools for Windows PowerShell)

Interface de rede

Para visualizar o nome de host DNS privado para uma interface de rede por meio do console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede na lista.
4. No painel de detalhes, o campo Private DNS (IPv4) DNS privado (IPv4) exibe o nome do host DNS privado.

Para visualizar nomes de host DNS para uma interface de rede por meio da linha de comando

- describe-network-interfaces (AWS CLI)
- Get-EC2NetworkInterface (AWS Tools for Windows PowerShell)

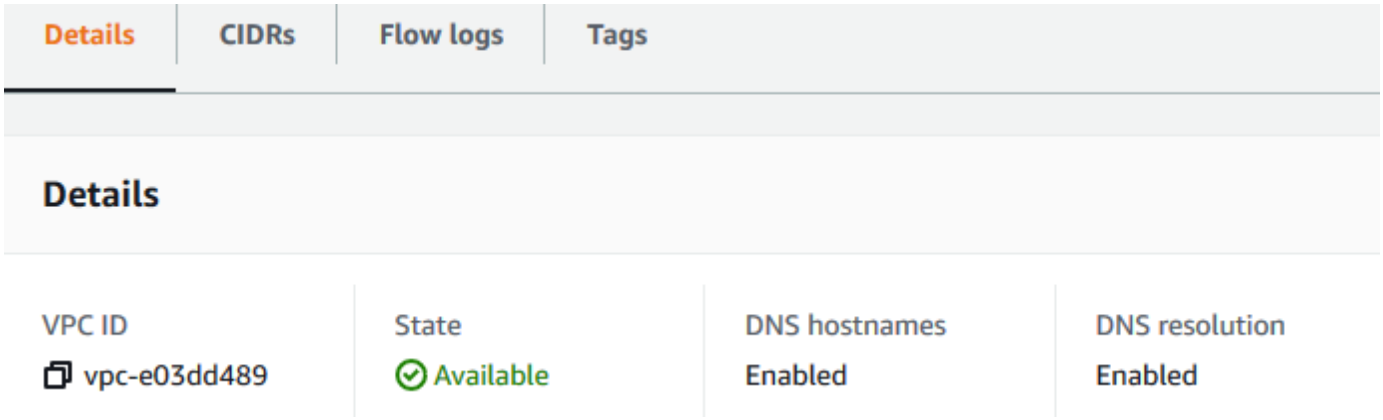
Exibir e atualizar atributos DNS para sua VPC

É possível visualizar e atualizar os atributos de suporte a DNS para a VPC usando o console da Amazon VPC. Essas configurações controlam se suas instâncias recebem nomes de host DNS públicos e se o servidor Amazon DNS pode resolver seus nomes DNS privados. Configurar esses atributos corretamente é vital para garantir uma comunicação perfeita em sua VPC.

Para descrever e atualizar o suporte a DNS para uma VPC por meio do console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Marque a caixa de seleção da VPC.

4. Revise as informações em Details (Detalhes). Nesse exemplo, as opções DNS hostnames (Nomes de hosts DNS) e DNS Resolution (Resolução de DNS) estã habilitadas.



5. Para atualizar essas configurações, escolha Actions (Ações) e, em seguida, Edit VPC settings (Editar configurações da VPC). Marque ou desmarque Enable (Habilitar) no atributo do DNS apropriado e escolha Save changes (Salvar alterações).

Para descrever um suporte a DNS para uma VPC por meio da linha de comando

- describe-vpc-attribute (AWS CLI)
- Get-EC2VpcAttribute (AWS Tools for Windows PowerShell)

Para atualizar um suporte a DNS para uma VPC por meio da linha de comando

- modify-vpc-attribute (AWS CLI)
- Edit-EC2VpcAttribute (AWS Tools for Windows PowerShell)

Uso de endereço de rede para sua VPC

O uso de endereço de rede (NAU) é uma métrica aplicada aos recursos da sua rede virtual para ajudar você a planejar e monitorar o tamanho da sua VPC. Cada unidade de NAU contribui para um total que representa o tamanho da sua VPC.

É importante entender o número total de unidades que compõem o NAU da sua VPC porque as seguintes cotas de VPC limitam o tamanho de uma VPC:

- Uso do endereço de rede: o número máximo de unidades de NAU que uma única VPC pode ter. Cada VPC pode ter até 64.000 unidades de NAU, por padrão. É possível solicitar um aumento da cota de até 256.000.
- Uso de endereços de rede emparelhados: o número máximo de unidades de NAU para uma VPC e todas as suas VPCs emparelhadas. Se uma VPC for emparelhada com outras VPCs na mesma região, as VPCs combinadas poderão ter até 128.000 unidades de NAU, por padrão. É possível solicitar um aumento da cota de até 512.000. VPCs que estão emparelhadas em diferentes regiões não contribuem para esse limite.

Você pode usar o NAU das seguintes maneiras:

- Antes de criar sua rede virtual, calcule as unidades de NAU para ajudar você a decidir se deve distribuir workloads por várias VPCs.
- Depois de criar sua VPC, use o Amazon CloudWatch para monitorar o uso do NAU da VPC para que ela não cresça além dos limites da cota do NAU. Para ter mais informações, consulte the section called “Métricas do CloudWatch”.

Como o NAU é calculado

Se você entender como o NAU é calculado, ele poderá ajudar você a planejar a escalabilidade das suas VPCs.

A tabela a seguir explica quais recursos compõem a contagem do NAU em uma VPC e quantas unidades de NAU cada recurso usa. Alguns recursos da AWS são representados como unidades de NAU únicas e alguns recursos são representados como várias unidades de NAU. Você pode usar a tabela para saber como o NAU é calculado.

Recurso	Unidades de NAU
Cada endereço IPv4 privado ou público e cada IPv6 atribuído a uma interface de rede para uma instância do EC2 na VPC	1
Interfaces de rede adicionais anexadas a uma instância do EC2	1
Prefixos de endereço IP atribuídos a uma interface de rede	1
Network Load Balancer por AZ	6

Recurso	Unidades de NAU
Gateway Load Balancer por AZ	6
Endpoint da VPC por AZ	6
Anexo do gateway de trânsito	6
Função do Lambda	6
nat gateway	6
Alvo de montagem do EFS	6
Interface EFA (EFA com um dispositivo ENA) ou uma interface somente EFA	1
Pod do Amazon EKS	1

Exemplos de NAU

Os exemplos a seguir mostram como calcular o NAU.

Exemplo 1: duas VPCs conectadas usando emparelhamento de VPC

VPCs emparelhadas na mesma região contribuem para uma cota combinada do NAU.

- VPC 1
  - 50 Network Load Balancers em duas sub-redes em zonas de disponibilidade separadas: 600 unidades de NAU
  - 5.000 instâncias (cada uma com endereço IPv4 e endereço IPv6) em uma sub-rede e 5.000 instâncias (cada uma com endereço IPv4 e endereço IPv6) em outra sub-rede: 20.000 unidades
  - 100 funções do Lambda: 600 unidades de NAU
- VPC 2
  - 50 Network Load Balancers em duas sub-redes em zonas de disponibilidade separadas: 600 unidades de NAU
  - 5.000 instâncias (cada uma com endereço IPv4 e endereço IPv6) em uma sub-rede e 5.000 instâncias (cada uma com endereço IPv4 e endereço IPv6) em outra sub-rede: 20.000 unidades

    - 100 funções do Lambda: 600 unidades de NAU
- Contagem total de NAU de emparelhamento: 42.400 unidades
- Cota padrão de NAU de emparelhamento: 128.000 unidades

Exemplo 2: duas VPCs conectadas usando um gateway de trânsito

As VPCs conectadas usando um gateway de trânsito não contribuem para uma cota combinada do NAU, como ocorre com as VPCs emparelhadas.

- VPC 1
    - 50 Network Load Balancers em duas sub-redes em zonas de disponibilidade separadas: 600 unidades de NAU
    - 5.000 instâncias (cada uma com endereço IPv4 e endereço IPv6) em uma sub-rede e 5.000 instâncias (cada uma com endereço IPv4 e endereço IPv6) em outra sub-rede: 20.000 unidades
    - 100 funções do Lambda: 600 unidades de NAU
- VPC 2
    - 50 Network Load Balancers em duas sub-redes em zonas de disponibilidade separadas: 600 unidades de NAU
    - 5.000 instâncias (cada uma com endereço IPv4 e endereço IPv6) em uma sub-rede e 5.000 instâncias (cada uma com endereço IPv4 e endereço IPv6) em outra sub-rede: 20.000 unidades
    - 100 funções do Lambda: 600 unidades de NAU
- Contagem total de NAU por VPC: 21.200 unidades
- Cota padrão de NAU por VPC: 64.000 unidades

Compartilhar as sub-redes da sua VPC com outras contas

O compartilhamento de sub-redes da VPC permite que várias Contas da AWS criem os próprios recursos de aplicação, como instâncias do Amazon EC2, bancos de dados do Amazon Relational Database Service (RDS), clusters do Amazon Redshift e funções do AWS Lambda, em nuvens privadas virtuais (VPCs) compartilhadas e gerenciadas centralmente. Nesse modelo, a conta que possui a VPC (proprietária) compartilha uma ou mais sub-redes com outras contas (participantes) que pertencem à mesma organização no AWS Organizations. Quando uma sub-rede é compartilhada, os participantes podem visualizar, criar, modificar e excluir os recursos de

seus aplicativos nas sub-redes compartilhadas com eles. Os participantes não poderão visualizar, modificar ou excluir recursos que pertencerem a outros participantes ou proprietários da VPC.

Você também pode compartilhar as sub-redes da VPC para aproveitar o roteamento implícito em uma VPC para aplicações que exijam um alto grau de interconectividade e que estejam dentro dos mesmos limites de confiança. Isso reduz o número de VPCs que você cria e gerencia, enquanto ainda usa contas separadas para faturamento e controle de acesso. Os clientes podem simplificar as topologias de rede interconectando sub-redes compartilhadas da Amazon VPC usando recursos de conectividade, como o AWS PrivateLink, gateways de trânsito e emparelhamento de VPCs. Para obter mais informações sobre os benefícios do compartilhamento de sub-redes da VPC, consulte VPC sharing: A new approach to multiple accounts and VPC management.

Há cotas relacionadas a compartilhamentos de sub-redes da VPC. Para ter mais informações, consulte compartilhamento sub-rede VPC.

Conteúdo

Pré-requisitos para sub-rede compartilhada

Esta seção contém os pré-requisitos para trabalhar com sub-redes compartilhadas:

- As contas de proprietário e participante da VPC devem ser gerenciadas pelo AWS Organizations.
- Você deve habilitar o compartilhamento de recursos no console do AWS RAM na conta de gerenciamento da sua organização. Para obter mais informações, consulte Habilitar o compartilhamento de recursos no AWS Organizations no Guia do usuário do AWS RAM.
- Você deve criar um compartilhamento de recursos. Você pode especificar as sub-redes a serem compartilhadas ao criar o compartilhamento de recursos ou pode adicionar as sub-redes ao compartilhamento de recursos posteriormente usando o procedimento descrito na próxima seção. Para obter mais informações, consulte Create a resource share no Guia do usuário do AWS RAM.

Trabalhando com sub-redes compartilhadas

Esta seção descreve como trabalhar com sub-redes compartilhadas no console da AWS e na AWS CLI.

Conteúdo

Compartilhar uma sub-rede

Você pode compartilhar sub-redes não padrão com outras contas da sua organização como explicado a seguir. Além disso, você pode compartilhar grupos de segurança entre organizações da AWS. Para ter mais informações, consulte Compartilhar grupos de segurança com o AWS Organizations.

Para compartilhar uma sub-rede usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Sub-redes.
3. Selecione sua sub-rede e escolha Actions (Ações), Share subnet (Compartilhar sub-rede).
4. Selecione seu compartilhamento de recurso e escolha Share subnet (Compartilhar sub-rede).

Para compartilhar uma sub-rede usando a AWS CLI

Use os comandos create-resource-share e associate-resource-share.

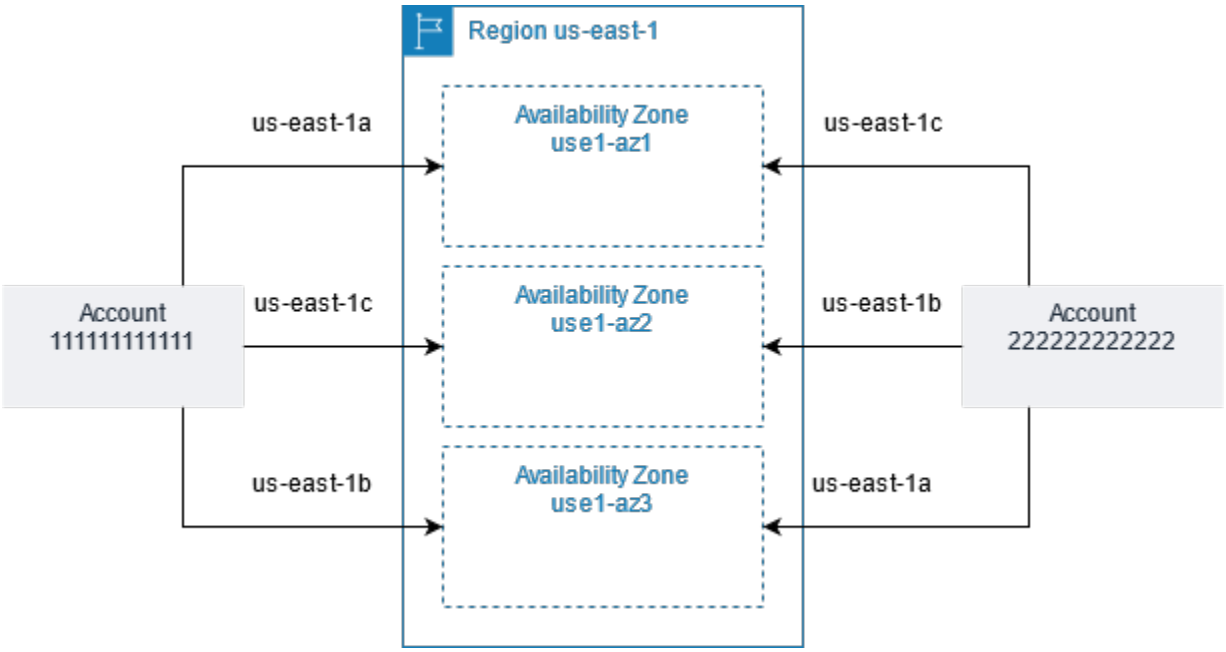
Mapear sub-redes entre zonas de disponibilidade

Para garantir a distribuição de recursos entre as zonas de disponibilidade de uma região, mapeamos as zonas de disponibilidade de forma independente para os nomes de cada conta. Por exemplo, a zona de disponibilidade `us-east-1a` de sua conta da AWS pode não ter o mesmo local que a `us-east-1a` de outra conta da AWS.

Para coordenar as zonas de disponibilidade entre contas para o compartilhamento de VPC, você deve usar um ID da zona de disponibilidade, que é um identificador exclusivo e consistente de uma zona de disponibilidade. Por exemplo, `use1-az1` é o ID de uma das zonas de disponibilidade

na região `us-east-1`. É possível visualizar os IDs de zona de disponibilidade para determinar o local dos recursos em uma conta em relação a outra conta. Você pode visualizar o ID da zona de disponibilidade de cada sub-rede no console da Amazon VPC.

O diagrama a seguir ilustra duas contas com diferentes mapeamentos de código de zona de disponibilidade para o ID de zona de disponibilidade.



Cancelar o compartilhamento de uma sub-rede compartilhada

O proprietário pode cancelar o compartilhamento de uma sub-rede com seus participantes em qualquer momento. Quando o proprietário cancela o compartilhamento de uma sub-rede compartilhada, as seguintes regras são aplicáveis:

- Os recursos existentes dos participantes continuarão em execução na sub-rede não compartilhada. Os serviços gerenciados da AWS (por exemplo, Elastic Load Balancing) que têm fluxos de trabalho automatizados/gerenciados (como auto scaling ou substituição de nós) podem exigir acesso contínuo à sub-rede compartilhada para alguns recursos.
- Os participantes não poderão mais criar novos recursos na sub-rede não compartilhada.
- Os participantes poderão modificar, descrever e excluir seus recursos que estiverem na sub-rede.
- Se os participantes ainda tiverem recursos na sub-rede não compartilhada, o proprietário não poderá excluir a sub-rede compartilhada ou a VPC da sub-rede compartilhada. O proprietário só poderá excluir a sub-rede ou a VPC da sub-rede compartilhada depois que os participantes excluírem todos os recursos da sub-rede não compartilhada.

Para cancelar o compartilhamento de uma sub-rede usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Sub-redes.
3. Selecione sua sub-rede e escolha Actions (Ações), Share subnet (Compartilhar sub-rede).
4. Escolha Actions (Ações), Stop sharing (Interromper compartilhamento).

Para cancelar o compartilhamento de uma sub-rede usando a AWS CLI

Use o comando disassociate-resource-share.

Identificar o proprietário de uma sub-rede compartilhada

Os participantes podem visualizar as sub-redes compartilhadas com eles usando o console da Amazon VPC ou a ferramenta da linha de comando.

Como identificar o proprietário de uma sub-rede usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Sub-redes. A coluna Owner (Proprietário) exibe o proprietário da sub-rede.

Para identificar o proprietário de uma sub-rede usando a AWS CLI

Use os comandos describe-subnets e describe-vpcs, que incluem o ID do proprietário em seus resultados.

Cobrança e medição para o proprietário e participantes

Esta seção contém detalhes de cobrança e medição para aqueles que possuem a sub-rede compartilhada e para aqueles que trabalham com a sub-rede compartilhada:

- Em uma VPC compartilhada, cada participante paga pelos recursos de aplicações, incluindo instâncias do Amazon EC2, bancos de dados do Amazon Relational Database Service, clusters do Amazon Redshift e funções do AWS Lambda. Os participantes também devem pagar pela transferência de dados realizada entre zonas de disponibilidade e pela transferência de dados via conexões de emparelhamento de VPC, entre gateways da Internet e entre gateways AWS Direct Connect.

- Os proprietários da VPC são cobrados por hora (onde aplicável), pelo processamento de dados e pela transferência de dados em todos os gateways NAT, gateways privados virtuais, gateways de trânsito, AWS PrivateLink e VPC endpoints. Além disso, os endereços IPv4 públicos usados em VPCs compartilhadas são cobrados dos proprietários de VPCs. Para obter mais informações sobre preços de endereços IPv4 públicos, consulte a guia Endereço IPv4 público na Página de preços da Amazon VPC.
- As transferências de dados dentro da mesma zona de disponibilidade (identificadas por seu ID de AZ exclusivo) são gratuitas, independentemente de quem é o proprietário dos recursos em comunicação.

Responsabilidades e permissões para proprietários e participantes

Esta seção inclui detalhes sobre as responsabilidades e permissões dos proprietários da sub-rede compartilhada (proprietário) e dos que estão usando a sub-rede compartilhada (participante).

Recursos dos proprietários

Os proprietários são responsáveis pelos recursos da VPC da qual são donos. Os proprietários da VPC são responsáveis por criar, gerenciar e excluir os recursos associados a uma VPC compartilhada. Isso inclui sub-redes, tabelas de rotas, ACLs de rede, conexões de emparelhamento, endpoints de gateway, endpoints de interface, endpoints do Amazon Route 53 Resolver, gateways da Internet, gateways NAT, gateways privados virtuais e anexos do transit gateway.

Recursos dos participantes

Os participantes são responsáveis pelos recursos da VPC dos quais são donos. Os participantes podem criar um conjunto limitado de recursos da VPC em uma VPC compartilhada. Por exemplo, os participantes podem criar interfaces de rede e grupos de segurança e habilitar logs de fluxo de VPC para as interfaces pertencentes a eles. Os recursos da VPC que um participante cria contam com base nas cotas da VPC na conta do participante, não na conta do proprietário. Para ter mais informações, consulte compartilhamento sub-rede VPC.

Recursos da VPC

As seguintes responsabilidades e permissões se aplicam aos recursos da VPC ao trabalhar com sub-redes de VPC compartilhadas:

Logs de fluxo

- Os participantes podem criar, excluir e descrever logs de fluxo de interfaces de rede de sua propriedade em uma sub-rede compartilhada da VPC.
- Os participantes não podem criar, excluir e descrever logs de fluxo de interfaces de rede que não sejam de sua propriedade em uma sub-rede compartilhada da VPC.
- Os participantes não podem criar, excluir ou descrever logs de fluxo em uma sub-rede compartilhada da VPC.
- Os proprietários da VPC podem criar, excluir e descrever logs de fluxo de interfaces de rede que não sejam de sua propriedade em uma sub-rede compartilhada da VPC.
- Os proprietários da VPC podem criar, excluir e descrever logs de uma sub-rede compartilhada da VPC.
- Os proprietários de VPC não podem descrever ou excluir logs de fluxo criados por um participante.

Gateways da Internet e gateways da Internet somente de saída

- Os participantes não podem criar, anexar ou excluir gateways da Internet e gateways da Internet somente de saída em uma sub-rede de VPC compartilhada. Os participantes podem descrever os gateways da Internet em uma sub-rede deVPC compartilhada. Os participantes não podem descrever gateways da Internet somente de saída em uma sub-rede de VPC compartilhada.

Gateways NAT

- Os participantes não podem criar, excluir ou descrever gateways NAT em uma sub-rede de VPC compartilhada.

Listas de controle de acesso à rede (NACLs)

- Os participantes não podem criar, excluir ou substituir NACLs em uma sub-rede de VPC compartilhada. Os participantes podem descrever NACLs criadas por proprietários de VPC em uma sub-rede de VPC compartilhada.

Interfaces de rede

- Os participantes podem criar interfaces de rede em uma sub-rede de VPC compartilhada. Os participantes não podem trabalhar com interfaces de rede criadas por proprietários de VPC em

uma sub-rede de VPC compartilhada de nenhuma outra forma, por exemplo, anexar, desanexar ou modificar as interfaces de rede. Os participantes podem modificar ou excluir as interfaces de rede que eles criaram em uma VPC compartilhada. Por exemplo, os participantes podem associar ou desassociar endereços IP com as interfaces de rede que eles criaram.

- Os proprietários de VPC podem descrever as interfaces de rede de propriedade dos participantes em uma sub-rede de VPC compartilhada. Os proprietários de VPC não podem trabalhar com interfaces de rede de propriedade dos participantes de nenhuma outra forma, por exemplo, anexar, desanexar ou modificar as interfaces de rede de propriedade dos participantes em uma sub-rede de VPC compartilhada.

Tabelas de rotas

- Os participantes não podem trabalhar com tabelas de rotas (por exemplo, criar, excluir ou associar tabelas de rotas) em uma sub-rede de VPC compartilhada. Os participantes podem descrever tabelas de rotas em uma sub-rede de VPC compartilhada.

Grupos de segurança

- Os participantes podem trabalhar com (criar, excluir, descrever, modificar ou criar regras de entrada e de saída para) grupos de segurança pertencentes a eles em uma sub-rede de VPC compartilhada. Os participantes poderão trabalhar com grupos de segurança criados pelos proprietários da VPC se o proprietário da VPC compartilhar o grupo de segurança com o participante.
- Os participantes podem criar regras nos grupos de segurança de sua propriedade que façam referência a grupos de segurança que pertençam a outros participantes ou ao proprietário da VPC da seguinte maneira: account-number/security-group-id
- Os participantes não podem executar instâncias usando o grupo de segurança padrão para a VPC porque ele pertence ao proprietário.
- Os participantes não podem iniciar instâncias usando grupos de segurança não padrão pertencentes ao proprietário da VPC ou a outros participantes a menos que o grupo de segurança seja compartilhado com eles.
- Os proprietários de VPC podem descrever os grupos de segurança criados pelos participantes em uma sub-rede de VPC compartilhada. Os proprietários de VPC pnão podem trabalhar com grupos de segurança criados por participantes de nenhuma outra forma. Por exemplo, proprietários de VPC não podem executar instâncias usando grupos de segurança criados por participantes.

Sub-redes

- Os participantes não podem modificar sub-redes compartilhadas ou os atributos relacionados. Somente o proprietário da VPC pode fazer isso. Os participantes podem descrever sub-redes em uma sub-rede de VPC compartilhada.
- Os proprietários de VPC podem compartilhar sub-redes apenas com outras contas ou unidades organizacionais que estão na mesma organização do AWS Organizations. Os proprietários de VPC não podem compartilhar sub-redes que estejam em uma VPC padrão.

Gateways de trânsito

- Somente o proprietário de VPC pode anexar um gateway de trânsito a uma sub-rede de VPC compartilhada. Os participantes não podem.

VPCs

- Os participantes não podem modificar VPCs ou os atributos relacionados. Somente o proprietário da VPC pode fazer isso. Os participantes podem descrever as VPCs, os atributos e os conjuntos de opções de DHCP.
- As tags da VPC e as tags para os recursos dentro da VPC compartilhada não são compartilhadas com os participantes.
- Os participantes podem associar seus próprios grupos de segurança a uma VPC compartilhada. Isso permite que o participante use o grupo de segurança com as interfaces de rede elásticas que ele possui na VPC compartilhada.

Recursos da AWS e sub-redes de VPC

Os Serviços da AWS listados nesta seção são compatíveis com os recursos nas sub-redes de VPC compartilhadas.

Para obter mais informações sobre como o serviço oferece suporte para as sub-redes de VPC compartilhadas, acesse os links para a documentação do serviço correspondente.

- Amazon Aurora
- AWS CodeBuild
- AWS Database Migration Service

- Amazon EC2
- Amazon ECS
- Amazon ElastiCache (Redis OSS)
- Amazon EFS
- Amazon Elastic Kubernetes Service
- Elastic Load Balancing
  - Application Load Balancers
  - Gateway Load Balancers
  - Network Load Balancers
- Amazon EMR
- AWS Glue
- AWS Lambda
- Amazon MQ executando o Apache MQ (não o Rabbit MQ)
- Amazon MSK
- AWS Network Manager
  - AWS Cloud WAN
  - Analisador de Acesso à Rede
  - Reachability Analyzer
- Amazon OpenSearch Service
- AWS PrivateLink†
- Amazon Relational Database Service (RDS)
- Amazon Redshift
- Amazon Route 53
- AWS Transit Gateway
- Acesso Verificado pela AWS
- Amazon VPC
  - Emparelhamento
  - Espelhamento de tráfego
- Amazon VPC Lattice

† Você pode se conectar a todos os serviços da AWS que oferecem suporte ao PrivateLink usando um endpoint de VPC em uma VPC compartilhada. Para obter uma lista de serviços que oferecem suporte ao PrivateLink, consulte Serviços da AWS que se integram ao AWS PrivateLink, no Guia do AWS PrivateLink.

A lista nesta seção representa nosso melhor esforço para documentar quais serviços são compatíveis com a inicialização de recursos em sub-redes da VPC compartilhada. Pode haver outros serviços não listados aqui que sejam compatíveis com a inicialização de recursos em sub-redes da VPC compartilhada. Recomendamos enviar feedback em caso de dúvidas sobre recursos que não estão nesta lista.

Estender uma VPC para uma zona local, zona Wavelength ou Outpost

É possível hospedar recursos da VPC, como sub-redes, em vários locais no mundo todo. Esses locais são compostos por regiões, zonas de disponibilidade, Local Zones e Wavelength Zones. Cada Região é uma área geográfica separada.

- As zonas de disponibilidade são vários locais isolados dentro de cada Região.
- O Local Zones permite colocar recursos, como computação e armazenamento, em vários locais mais próximos dos usuários finais.
- O AWS Outposts leva serviços, infraestrutura e modelos operacionais nativos da AWS a praticamente qualquer data center, espaço de colocalização ou on-premises.
- As zonas do Wavelength permitem que os desenvolvedores criem aplicações que oferecem baixíssimas latências para dispositivos 5G e usuários finais. O Wavelength implanta os serviços de armazenamento e computação padrão da AWS até a borda das redes 5G de operadoras de telecomunicação.

A AWS opera data centers de última geração com alta disponibilidade. Embora sejam raras, podem ocorrer falhas que afetam a disponibilidade das instâncias que estão no mesmo local. Se você hospedar todas as suas instâncias em um único local afetado por uma falha, nenhuma delas ficará disponível.

Sub-redes em AWS Local Zones

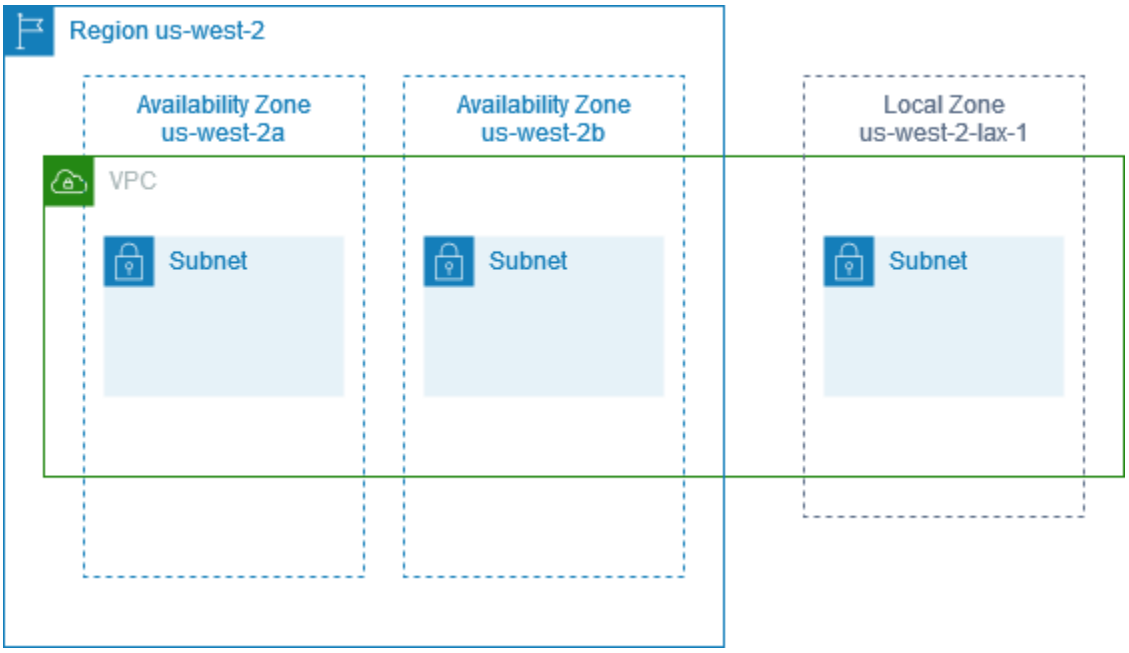
O AWS Local Zones permite colocar os recursos mais próximos dos usuários e estabelecer facilmente conexões para todos os serviços na Região da AWS usando APIs e conjuntos de

ferramentas bem conhecidos. Quando você cria uma sub-rede em uma zona local, sua VPC também é estendida para essa zona local.

Para usar uma zona local, siga este processo:

- Entre na zona local.
- Crie uma sub-rede na zona local.
- Selecione recursos na sub-rede da zona local para que suas aplicações fiquem mais próximas dos usuários.

O diagrama a seguir ilustra uma VPC na região Oeste dos EUA (Oregon) (`us-west-2`) que abrange zonas de disponibilidade e uma zona local.



Ao criar uma VPC, você pode optar por atribuir a ela um conjunto de endereços IP públicos fornecidos pela Amazon. Você também pode definir para os endereços um grupo de borda de rede que limite os endereços ao grupo. Quando você define um grupo de borda de rede, os endereços IP não podem se ser movidos entre os grupos de borda de rede. O tráfego de rede da zona local vai diretamente para a Internet ou para os pontos de presença (POPs) sem atravessar a região superior da zona local, permitindo acesso à computação de baixa latência. Para obter a lista completa de zonas locais e respectivas regiões acima, consulte Zonas locais disponíveis no Guia do usuário de zonas locais da AWS.

As regras a seguir se aplicam às Local Zones:

- As sub-redes da zona local seguem as mesmas regras de roteamento que a sub-rede da zona de disponibilidade, incluindo tabelas de rotas, grupos de segurança e ACLs de rede.
- O tráfego de saída da Internet deixa uma zona local do Local Zones.
- É necessário provisionar endereços IP públicos para uso em uma zona local. Ao alocar endereços, você pode especificar o local a partir do qual o endereço IP é anunciado. Chamamos isso de grupo de borda de rede, e é possível definir esse parâmetro para limitar os endereços a esse local. Após provisionar os endereços IP, não será possível movê-los entre a zona local e a Região pai (por exemplo, de `us-west-2-lax-1a` para `us-west-2`).
- Se a zona local é compatível com IPv6, é possível solicitar os endereços IP IPv6 fornecidos pela Amazon e associá-los ao grupo de borda de rede para uma VPC nova ou existente. Para obter a lista de zonas locais compatíveis com IPv6, consulte Considerações no Guia do usuário de zonas locais da AWS
- Não é possível criar endpoints da VPC dentro das sub-redes da zona local.

Para mais informações sobre como trabalhar com Local Zones, consulte o Guia do usuário do AWS Local Zones.

Considerações sobre gateways da Internet

Leve em consideração as seguintes informações ao usar gateways da Internet (na Região pai) no Local Zones:

- Você pode usar gateways da Internet no Local Zones com endereços IP elásticos ou endereços IP públicos atribuídos automaticamente pela Amazon. Os endereços IP elásticos associados devem incluir o grupo de borda de rede da zona local. Para obter mais informações, consulte the section called “Endereços IP elásticos”.

  Não é possível associar um endereço IP elástico definido para a Região.
- Os endereços IP elásticos usados no Local Zones têm as mesmas cotas que os endereços IP elásticos em uma Região. Para obter mais informações, consulte the section called “Endereços IP elásticos”.
- Você pode usar gateways da Internet em tabelas de rotas associadas aos recursos da zona local. Para obter mais informações, consulte the section called “Roteamento para um gateway da Internet”.

Acessar o Local Zones usando um gateway do Direct Connect

Considere o cenário em que você deseja que um data center on-premises acesse recursos que estão em uma zona local. Use um gateway privado virtual para a VPC associada à zona local para se conectar a um gateway do Direct Connect. O gateway do Direct Connect se conecta a um local do AWS Direct Connect em uma Região. O datacenter on-premises tem uma conexão do AWS Direct Connect com o local do AWS Direct Connect.

> **Note**
>
> O tráfego destinado a uma sub-rede em uma zona local usando o Direct Connect não passa pela região pai da zona local. Em vez disso, o tráfego segue o caminho mais curto até a zona local. Isso diminui a latência e ajuda a melhorar a resposta dos seus aplicativos.

Configure os seguintes recursos para esta configuração:

- Um gateway privado virtual para a VPC associada à sub-rede da zona Local. É possível visualizar a VPC para a sub-rede na página de detalhes da sub-rede no Amazon Virtual Private Cloud Console, ou usar o comando describe-subnets.

  Para obter informações sobre como criar um gateway privado virtual, consulte Criar um gateway de destino no Manual do usuário do AWS Site-to-Site VPN.
- Uma conexão do Direct Connect. Para obter a melhor performance de latência, a AWS recomenda que você use a localidade do Direct Connect mais próxima da zona local para a qual você estará ampliando sua sub-rede.

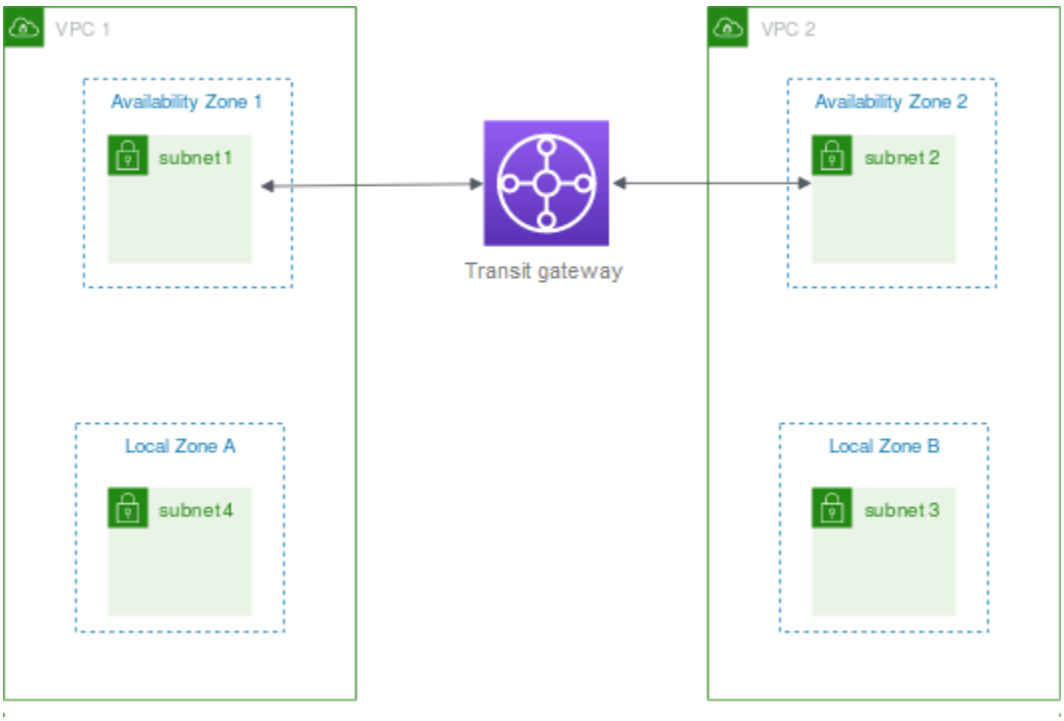
  Para obter informações sobre como solicitar uma conexão, consulte Conexões cruzadas no Manual do usuário do AWS Direct Connect.
- Gateway Direct Connect Para obter informações sobre como criar um gateway do Direct Connect, consulte Criação de um gateway do Direct Connect no Manual do usuário do AWS Direct Connect.
- Uma associação de gateway privado virtual para conectar a VPC ao gateway do Direct Connect. Para obter informações sobre como criar uma associação de gateway privado virtual, consulte Associação e desassociação de gateways privados virtuais no Manual do usuário do AWS Direct Connect.
- Uma interface virtual privada na conexão do local do AWS Direct Connect ao data center on-premises. Para obter informações sobre como criar um gateway do Direct Connect, consulte

Criação de uma interface virtual privada para o gateway do Direct Connect no Manual do usuário do AWS Direct Connect.

Conectar sub-redes do Local Zones a um gateway de trânsito

Não é possível criar um anexo do Transit Gateway para uma sub-rede em uma Zona local. O diagrama a seguir mostra como configurar a rede para que as sub-redes na zona local se conectem a um transit gateway por meio da Zona de disponibilidade principal. Crie sub-redes nas Local Zones e sub-redes nas Zonas de Disponibilidade principais. Conecte as sub-redes nas Zonas de disponibilidade principais ao transit gateway e crie uma rota na tabela de rotas para cada VPC que roteia o tráfego destinado para o CIDR da outra VPC para a interface de rede para o anexo do transit gateway.

> **Note**
>
> O tráfego destinado a uma sub-rede de uma zona local originário de um gateway de trânsito atravessará primeiro a região pai.



Crie os seguintes recursos para este cenário:

- Uma sub-rede em cada zona de disponibilidade principal. Para ter mais informações, consulte the section called “Criar uma sub-rede”.
- Um gateway de trânsito Para obter mais informações, consulte Criar um transit gateway em Amazon VPC Transit Gateways.
- Um anexo de transit gateway para a VPC usando a zona de disponibilidade principal. Para obter mais informações, consulte Criar um anexo de transit gateway para um VPC em Amazon VPC Transit Gateways.
- Uma tabela de rotas do gateway de trânsito associada a um anexo de gateway de trânsito. Para obter mais informações, consulte Tabelas de rota de Transit gateway em Amazon VPC Transit Gateway.
- Para cada VPC, uma entrada na tabela de rotas de sub-rede das sub-redes da zona local que têm outro CIDR de VPC como destino e o ID da interface de rede para o anexo do gateway de trânsito como alvo. Para localizar a interface de rede para o anexo do transit gateway, pesquise nas descrições das interfaces de rede o ID do anexo do transit gateway. Para ter mais informações, consulte the section called “Roteamento para um gateway de trânsito”.

Veja a seguir um exemplo de tabela de rotas para VPC 1.

Destino	Alvo
CIDR da VPC 1	*local*
CIDR da VPC 2	*vpc1-attachment-network-interface-id*

Veja a seguir um exemplo de tabela de rotas para VPC 2.

Destino	Alvo
CIDR da VPC 2	*local*
CIDR da VPC 1	*vpc2-attachment-network-interface-id*

Veja a seguir um exemplo da tabela de rotas de gateway de trânsito. Os blocos CIDR de cada VPC se propagam para a tabela de rotas do gateway de trânsito.

CIDR	Attachment	Tipo de rota
CIDR da VPC 1	*Anexo para a VPC 1*	com propagação
CIDR da VPC 2	*Anexo para a VPC 2*	com propagação

Sub-redes no AWS Wavelength

AWS Wavelength O permite que os desenvolvedores criem aplicativos que oferecem baixíssimas latências para dispositivos móveis e usuários finais. O Wavelength implanta os serviços de armazenamento e computação padrão da AWS até a borda das redes 5G de operadoras de telecomunicação. Os desenvolvedores podem estender uma nuvem privada virtual (VPC) para uma ou mais zonas do Wavelength e usar os recursos da AWS, como instâncias do Amazon EC2, para executar aplicações que exigem baixíssima latência e uma conexão com Serviços da AWS na região.

Para usar uma zona do Wavelength, primeiro é necessário escolher a zona. Em seguida, crie uma sub-rede na zona do Wavelength. É possível criar instâncias do Amazon EC2, volumes do Amazon EBS e sub-redes e gateways de operadora da Amazon VPC em zonas do Wavelength. Também é possível usar serviços que orquestram ou funcionam com o EC2, o EBS e a VPC, como o Amazon EC2 Auto Scaling, clusters do Amazon EKS, clusters do Amazon ECS, o Amazon EC2 Systems Manager, o Amazon CloudWatch, o AWS CloudTrail e o AWS CloudFormation. Os serviços no Wavelength são parte de uma VPC conectada por meio de uma conexão confiável de alta largura de banda a uma Região da AWS para facilitar o acesso a serviços, incluindo o Amazon DynamoDB e o Amazon RDS.

As seguintes regras se aplicam às zonas do Wavelength:

- Uma VPC se estende a uma zona do Wavelength quando você cria uma sub-rede na VPC e a associa à zona do Wavelength.
- Por padrão, cada sub-rede criada em uma VPC que abrange uma zona do Wavelength herda a tabela de rotas principal da VPC, incluindo a rota local.

- Ao executar uma instância do EC2 em uma sub-rede em uma zona do Wavelength, você atribui um endereço IP da operadora a ela. O gateway de operadora usa o endereço para o tráfego da interface para a Internet ou para dispositivos móveis. O gateway de operadora usa NAT para traduzir o endereço e envia o tráfego para o destino. Tráfego das rotas da rede da operadora de telecomunicações por meio do gateway de operadora.
- É possível definir o destino de uma tabela de rotas da VPC ou uma tabela de rotas da sub-rede em uma zona do Wavelength para um gateway de operadora, o que permite o tráfego de entrada de uma rede de operadora em um local específico e o tráfego de saída para a rede da operadora e a Internet. Para obter mais informações sobre opções de roteamento em uma zona do Wavelength, consulte Routing (Roteamento) no Guia do Desenvolvedor do AWS Wavelength.
- As sub-redes em zonas do Wavelength têm os mesmos componentes de rede que as sub-redes nas zonas de disponibilidade, incluindo endereços IPv4, conjuntos de opções DHCP e ACLs da rede.
- Não é possível criar um anexo do Transit Gateway para uma sub-rede em uma zona do Wavelength. Em vez disso, crie o anexo através de uma sub-rede na zona de disponibilidade pai e encaminhe o tráfego para os destinos desejados via gateway de trânsito. Consulte a próxima seção para ver um exemplo.

Considerações sobre várias zonas do Wavelength

As instâncias do EC2 que estão em zonas diferentes do Wavelength na mesma VPC não têm permissão para se comunicar entre si. Se você precisar de comunicação entre as zonas do Wavelength, a AWS recomenda que o uso de várias VPCs, uma para cada zona do Wavelength. É possível usar um gateway de trânsito para conectar as VPCs. Essa configuração permite a comunicação entre instâncias nas zonas do Wavelength.

O tráfego entre as zonas do Wavelength é roteado pela Região da AWS. Para obter mais informações, consulte AWS Transit Gateway.

O diagrama a seguir mostra como configurar a rede para que instâncias em duas zonas do Wavelength possam se comunicar. Você tem duas zonas do Wavelength (zona do Wavelength A e zona do Wavelength B). É necessário criar os seguintes recursos para habilitar a comunicação:

- Para cada zona de comprimento de onda, uma sub-rede em uma zona de disponibilidade pai da zona do Wavelength. No exemplo, você cria a sub-rede 1 e a sub-rede 2. Para obter informações sobre a criação de sub-redes, consulte the section called “Criar uma sub-rede”. Use o comando describe-availability-zones para encontrar a zona principal.

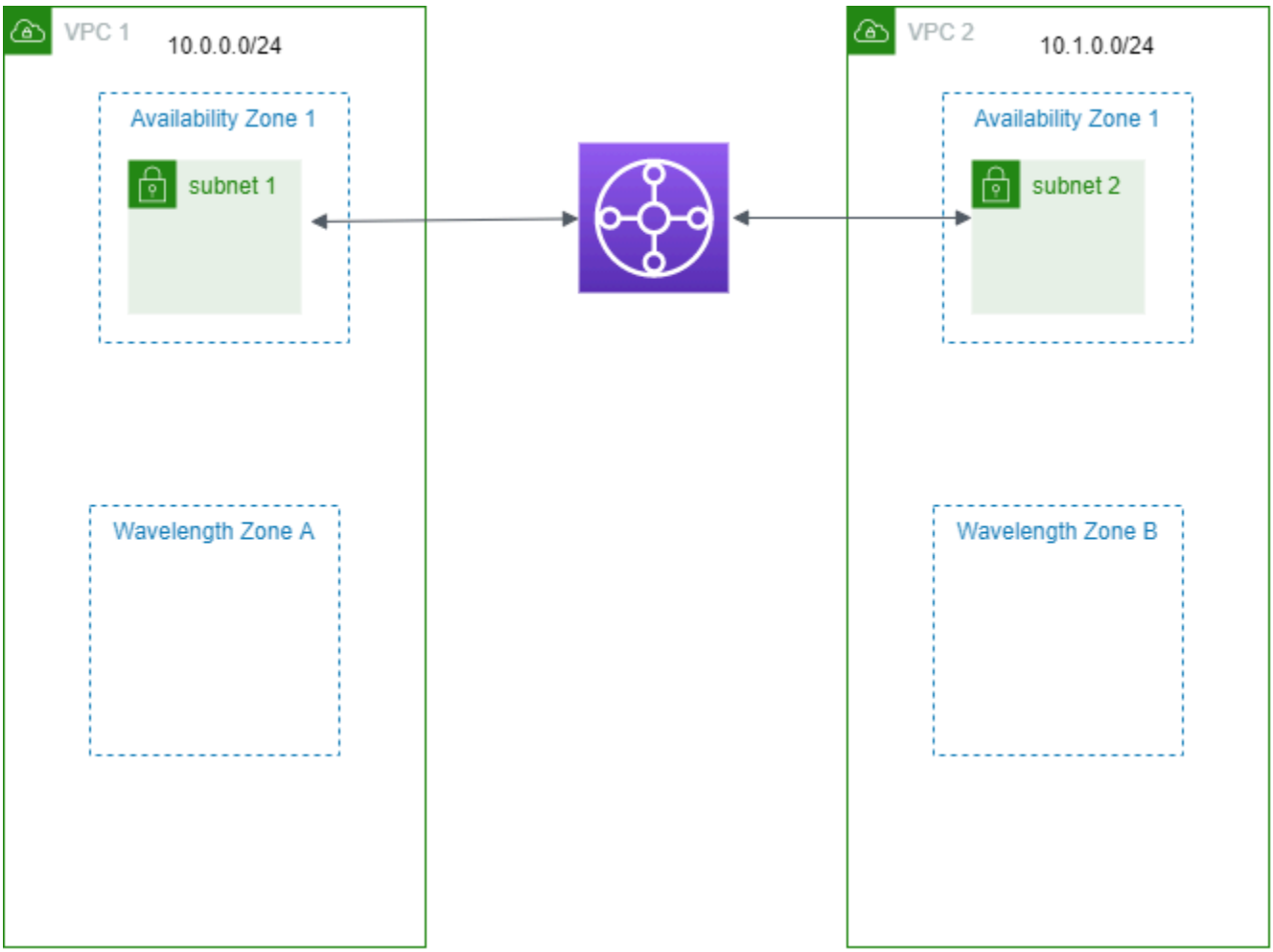
- Um gateway de trânsito O gateway de trânsito conecta as VPCs. Para obter informações sobre como criar um gateway de trânsito, consulte Criação de um gateway de trânsito no Guia do Amazon VPC Transit Gateways.
- Para cada VPC, um anexo da VPC ao gateway de trânsito na zona de disponibilidade pai da zona do Wavelength. Para obter mais informações, consulte Anexos do transit gateway para uma VPC no Manual do usuário do Amazon VPC Transit Gateway.
- Entradas para cada VPC na tabela de rotas do gateway de trânsito. Para obter informações sobre como criar rotas de gateway de trânsito, consulte Tabelas de rotas de gateway de trânsito no Guia do Amazon VPC Transit Gateways.
- Para cada VPC, uma entrada na tabela de rotas da VPC que tem o CIDR da outra VPC como destino e o ID do gateway de trânsito como destino. Para obter mais informações, consulte the section called “Roteamento para um gateway de trânsito”.

  No exemplo, a tabela de rotas para a VPC 1 tem a seguinte entrada:

Destino	Destino
10.1.0.0/24	tgw-22222222222222222

A tabela de rotas da VPC 2 tem a seguinte entrada:

Destino	Destino
10.0.0.0/24	tgw-22222222222222222



Sub-redes no AWS Outposts

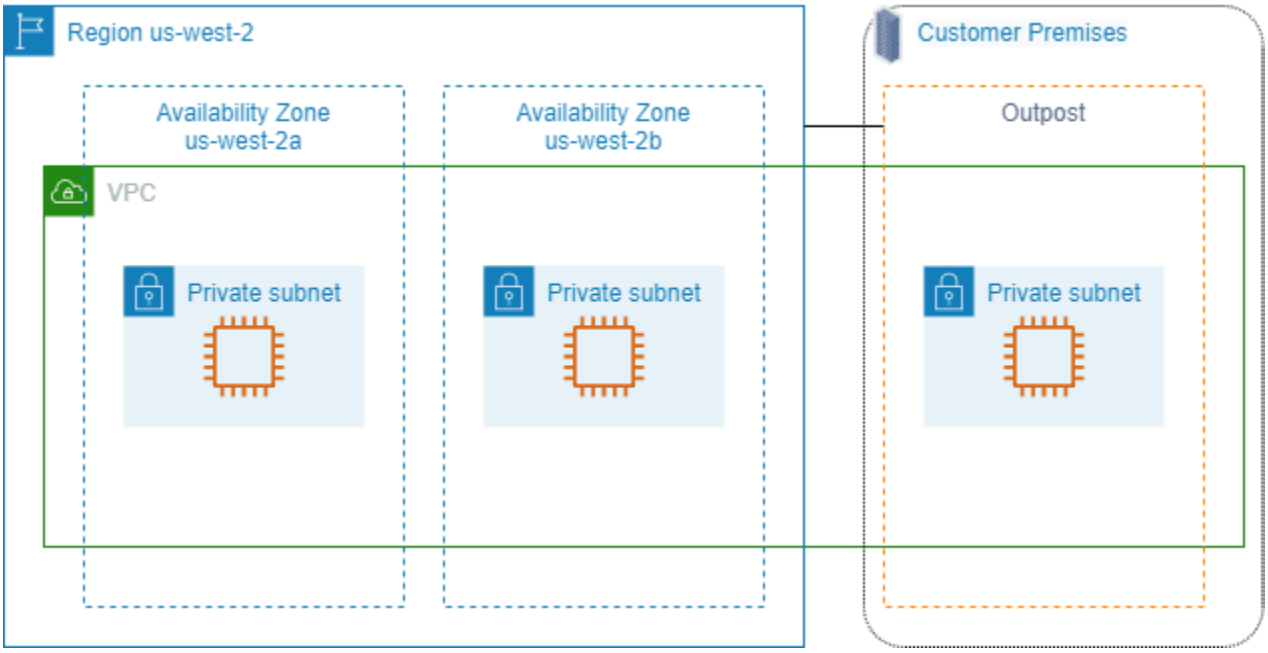
O AWS Outposts oferece a você os mesmos serviços, infraestrutura de hardware, APIs e ferramentas da AWS para criar e executar suas aplicações on-premises e na nuvem. O AWS Outposts é ideal para workloads que precisam de acesso de baixa latência a aplicações ou sistemas on-premises e a workloads que precisam armazenar e processar dados localmente. Para obter mais informações sobre o AWS Outposts, consulte AWS Outposts.

Uma VPC abrange todas as zonas de disponibilidade em uma região da AWS. Depois de conectar seu Outpost à região principal, você pode estender qualquer VPC na região para seu Outpost criando uma sub-rede para o Outpost nessa VPC.

As seguintes regras se aplicam ao AWS Outposts:

- As sub-redes devem residir em um local do Outpost.

- Você pode criar uma sub-rede para um Outpost ao especificar o nome do recurso da Amazon (ARN) do Outpost ao criar a sub-rede.
- Rack Outposts: um gateway local lida com a conectividade de rede entre a VPC e as redes on-premises. Para obter mais informações, consulte Gateways locais no Guia do usuário do AWS Outposts para racks Outposts.
- Servidores Outposts: uma interface de rede local lida com a conectividade de rede entre a VPC e as redes on-premises. Para obter mais informações, consulte Interfaces de rede local no Guia do usuário do AWS Outposts para servidores Outposts.
- Por padrão, cada sub-rede criada em uma VPC, incluindo sub-redes dos seus Outposts, é implicitamente associada à tabela de rotas principal da VPC. Você também pode associar explicitamente uma tabela de rotas personalizada às sub-redes em sua VPC e ter um gateway local como destino de próximo salto para todo o tráfego destinado à sua rede on-premises.



Excluir a VPC:

Quando não precisar mais de uma VPC, você poderá excluí-la.

Requisito

Para poder excluir uma VPC, você deve primeiro terminar ou excluir os recursos que criaram uma interface de rede gerenciada pelo solicitante na VPC. Por exemplo, você deve terminar as instâncias

do EC2 e excluir os balanceadores de carga, gateways NAT, anexos de VPC de gateways de trânsito e endpoints da VPC de interface.

> **Note**
>
> Se você criou um log de fluxo para a VPC que está excluindo, observe que os logs de fluxo das VPCs excluídas acabam sendo removidos automaticamente.

Conteúdo

Para excluir uma VPC usando o console

Se você excluir uma VPC usando o console da Amazon VPC, também excluímos os seguintes componentes da VPC para você:

- Opções do DHCP
- Gateways da Internet apenas de saída
- Endpoints de gateway
- Gateways da Internet
- Network ACLs
- Tabelas de rotas
- Grupos de segurança
- Sub-redes

Para excluir a VPC usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Termine todas as instâncias na VPC. Para obter mais informações, consulte Encerramento de instâncias no Guia do usuário do Amazon EC2.
3. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
4. No painel de navegação, escolha Your VPCs (Suas VPCs).
5. Selecione a VPC para excluir e escolha Ações, Excluir VPC.

6. Se houver recursos que precisem ser excluídos ou terminar antes que a VPC possa ser excluída, nós os exibiremos. Exclua ou termine esses recursos e, em seguida, tente novamente. Caso contrário, exibiremos os recursos que excluiremos além da VPC. Reveja a lista e avance para a próxima etapa.
7. (Opcional) Se você tiver uma conexão Site-to-Site VPN, selecione a opção para excluí-la. Caso planeje usar o gateway do cliente com outra VPC, recomendamos que você mantenha a conexão Site-to-Site VPN e os gateways. Caso contrário, será necessário configurar o dispositivo de gateway do cliente novamente depois que você criar uma nova conexão Site-to-Site VPN.
8. Quando a confirmação for solicitada, insira **`delete`** e selecione Excluir.

Excluir uma VPC usando a linha de comando

Para poder excluir uma VPC usando a linha de comando, você deve terminar ou excluir quaisquer recursos que criaram uma interface de rede gerenciada pelo solicitante na VPC. Você também deve terminar ou desvincular todos os recursos da VPC criados, como sub-redes, grupos de segurança, ACLs de rede, tabelas de rotas, gateways da Internet e gateways da Internet somente de saída. Não é necessário excluir o grupo de segurança padrão, a tabela de rotas padrão e a ACL de rede padrão.

O procedimento a seguir demonstra os comandos usados para excluir recursos da VPC comuns e, em seguida, excluir sua VPC. Você deve usar estes comandos nesta ordem. Se você criou recursos da VPC adicionais, também precisará usar o comando de exclusão correspondente antes de excluir a VPC.

Para excluir uma VPC usando a AWS CLI

1. Exclua seu grupo de segurança usando o comando delete-security-group.

```
aws ec2 delete-security-group --group-id sg-id
```

2. Exclua cada ACL de rede usando o comando delete-network-acl.

```
aws ec2 delete-network-acl --network-acl-id acl-id
```

3. Exclua cada sub-rede usando o comando delete-subnet.

```
aws ec2 delete-subnet --subnet-id subnet-id
```

4. Exclua cada tabela de rotas personalizada usando o comando delete-route-table.

```
aws ec2 delete-route-table --route-table-id rtb-id
```

5. Desanexe o gateway da Internet da sua VPC usando o comando detach-internet-gateway.

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-id --vpc-id vpc-id
```

6. Exclua seu gateway da Internet usando o comando delete-internet-gateway.

```
aws ec2 delete-internet-gateway --internet-gateway-id igw-id
```

7. [VPC de pilha dupla] Exclua seu gateway da Internet somente de saída usando o comando delete-egress-only-internet-gateway.

```
aws ec2 delete-egress-only-internet-gateway --egress-only-internet-gateway-id eigw-id
```

8. Exclua sua VPC usando o comando delete-vpc.

```
aws ec2 delete-vpc --vpc-id vpc-id
```

Gerar infraestrutura como código com base nas ações do seu console VPC usando o Console-to-Code

O console oferece um caminho guiado para criar recursos e testar protótipos. Se quiser criar os mesmos recursos em escala, você precisará de um código de automação. O Console-to-Code é um atributo do Amazon Q Developer que pode ajudar você a começar a usar seu código de automação. O Console-to-Code registra as ações que você faz no console, incluindo os valores padrão e os parâmetros compatíveis. Em seguida, a IA generativa é usada para sugerir código no formato de infraestrutura como código (IaC) de sua preferência para as ações desejadas. Como o fluxo de trabalho do console garante que os valores dos parâmetros que você especifica sejam válidos juntos, o código que você gera usando o Console-to-Code tem valores de parâmetros compatíveis. Você pode usar o código como ponto de partida e, depois, personalizá-lo para deixá-lo pronto para produção no seu caso de uso específico.

Por exemplo, com o Console-to-Code, você pode gravar suas ações usando o console VPC para criar sub-redes, grupos de segurança, NACLs, uma tabela de roteamento personalizada e um

gateway da internet e gerar código no formato JSON do AWS CloudFormation. Em seguida, você pode copiar esse código e personalizá-lo para uso em seu modelo do AWS CloudFormation.

Atualmente, o Console-to-Code pode gerar infraestrutura como código (IaC) nos seguintes formatos e linguagens:

- Java do CDK
- Python do CDK
- TypeScript do CDK
- JASON do CloudFormation
- YAML do CloudFormation

Para obter mais informações e instruções sobre como usar o Console-to-Code, consulte Automatizar serviços da AWS com o Console-to-Code do Amazon Q Developer no Guia do usuário do Amazon Q Developer.

Sub-redes para sua VPC

Uma sub-rede consiste em um intervalo de endereços IP na VPC. É possível criar recursos da AWS, como instâncias do EC2, em sub-redes específicas.

Conteúdo

Conceitos básicos sobre sub-redes

Cada sub-rede deve residir inteiramente dentro de uma zona de disponibilidade e não pode abranger zonas. Ao iniciar recursos da AWS em zonas de disponibilidade separadas, é possível proteger suas aplicações contra a falha de uma única zona de disponibilidade.

Conteúdo

Intervalo de endereços IP da sub-rede

Ao criar uma sub-rede, especifique seus endereços IP, dependendo da configuração da VPC:

- Somente IPv4: a sub-rede tem um bloco CIDR IPv4, mas não um bloco CIDR IPv6. Os recursos de uma sub-rede apenas IPv4 devem se comunicar via IPv4.
- Pilha dupla: a sub-rede tem um bloco CIDR IPv4 e um bloco CIDR IPv6. É necessário que a VPC tenha um bloco CIDR IPv4 e um bloco CIDR IPv6. Os recursos de uma sub-rede de dupla pilha conseguem se comunicar via IPv4 e IPv6.
- Somente IPv6: a sub-rede tem um bloco CIDR IPv6, mas não um bloco CIDR IPv4. A VPC deve ter um bloco CIDR IPv6. Os recursos de uma sub-rede apenas IPv6 devem se comunicar via IPv6.

> **Note**
>
> Os recursos em sub-redes que operam exclusivamente com a versão IPv6 são atribuídos a endereços IPv4 locais de link do bloco CIDR 169.254.0.0/16. Esses endereços são usados para a comunicação com os serviços que estão disponíveis somente na VPC. Para obter exemplos, consulte a seção Endereços locais de link no Guia do usuário do Amazon EC2.

Para ter mais informações, consulte Endereçamento IP para suas VPCs e sub-redes.

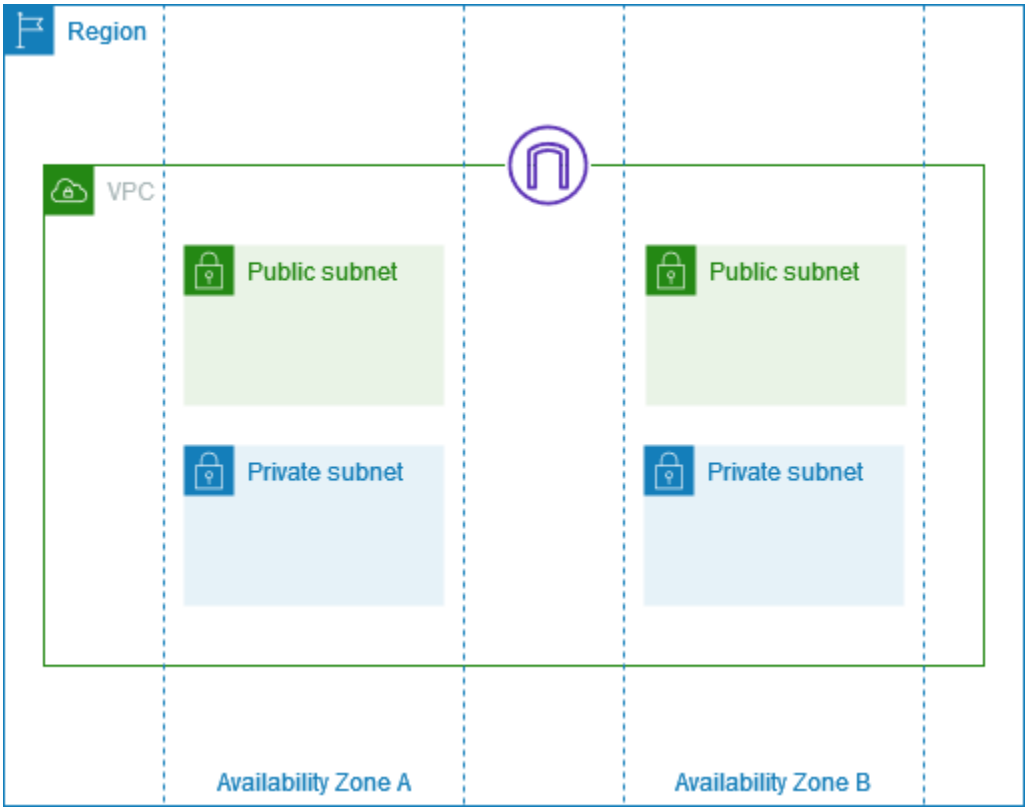
Tipos de sub-redes

O tipo de sub-rede é determinado pela forma como você configura o roteamento para suas sub-redes. Por exemplo:

- Sub-rede pública: a sub-rede tem uma rota direta para um gateway da Internet. Os recursos em uma sub-rede pública podem acessar a Internet pública.
- Sub-rede privada: a sub-rede não tem uma rota direta para um gateway da Internet. Os recursos em uma sub-rede privada exigem um dispositivo NAT para acessar a Internet pública.
- Sub-rede somente VPN: o tráfego da sub-rede é roteado para uma conexão do Site-to-Site VPN através de um gateway virtual privado. A sub-rede deve ter uma rota para um gateway da Internet.
- Sub-rede isolada: a sub-rede não tem rotas para destinos fora de sua VPC. Os recursos em uma sub-rede isolada só podem acessar ou ser acessados por outros recursos na mesma VPC.

Diagrama de sub-rede

O diagrama apresentado a seguir mostra uma VPC com sub-redes distribuídas em duas zonas de disponibilidade e um gateway da Internet. Em cada zona de disponibilidade, há uma sub-rede pública e uma sub-rede privada.



Para obter diagramas que mostram sub-redes em zonas locais e em zonas de comprimento de onda, consulte How AWS Local Zones work e How AWS Wavelength works.

Roteamento de sub-rede

Cada sub-rede deve estar associada a uma tabela de rotas, que especifica as rotas permitidas para o tráfego de saída deixando a sub-rede. Cada sub-rede que você cria é automaticamente associada à tabela de rotas principal da VPC. Você pode alterar a associação e o conteúdo da tabela de rotas principal. Para ter mais informações, consulte Configurar tabelas de rotas.

Configurações de sub-redes

Todas as sub-redes têm um atributo modificável que determina se uma interface de rede criada nesta sub-rede recebe um endereço IPv4 público e, se aplicável, um endereço IPv6. Isso inclui a interface de rede primária (por exemplo, eth0), que é criada para uma instância quando você a inicia nessa sub-rede. Independentemente do atributo da sub-rede, você ainda pode substituir esta configuração para uma instância específica durante a inicialização.

Após criar uma sub-rede, é possível modificar as seguintes configurações de sub-rede:

- Auto-assign IP settings (Atribuir configurações de IP automaticamente): esta opção permite que você defina a atribuição automática das configurações de IP para solicitar automaticamente um endereço IPv4 ou IPv6 público para uma nova interface de rede nesta sub-rede.
- Configurações de nomes baseados em recursos (RBN): permitem que você especifique o tipo de nome do host para as instâncias do EC2 nesta sub-rede e configure como as consultas de registros DNS A e AAAA são geridas. Para obter mais informações, consulte Tipos de nomes do host de instâncias do Amazon EC2 no Guia do usuário do Amazon EC2.

Segurança de sub-rede

Para proteger seus recursos da AWS, recomendamos o uso de sub-redes privadas. Use um bastion host ou dispositivo NAT para acesso à Internet em recursos, como instâncias do EC2, em uma sub-rede privada.

A AWS fornece recursos que você pode usar para aumentar a segurança dos recursos da VPC. Os grupos de segurança permitem o tráfego de recursos associados, como instâncias do EC2. ACLs de rede permitem ou recusam o tráfego de entrada e saída em nível de sub-rede. Na maioria dos casos, os grupos de segurança podem atender às suas necessidades. No entanto, você poderá usar as ACLs de rede se desejar uma camada adicional de segurança para a VPC. Para ter mais informações, consulte the section called “Comparar grupos de segurança e ACLs de rede”.

Por design, cada sub-rede deve estar associada a uma ACL de rede. Toda sub-rede que você cria é automaticamente associada à ACL padrão de rede para a VPC. A ACL de rede padrão permite todo o tráfego de entrada e saída. Você pode atualizar a ACL de rede padrão ou criar ACL de rede personalizadas e associá-las às suas sub-redes. Para ter mais informações, consulte Controlar o tráfego da sub-rede com listas de controle de acesso à rede.

Você pode criar um log de fluxo em sua VPC ou sub-rede para capturar o tráfego que entra e sai das interfaces de rede em sua VPC ou sub-rede. Você também pode criar um log de fluxo em uma interface de rede individual. Para ter mais informações, consulte Como registrar tráfego IP em log com logs de fluxo da VPC.

Criar uma sub-rede

Use os procedimentos a seguir para criar sub-redes para sua nuvem privada virtual (VPC). Dependendo da conectividade de que você precisa, talvez também seja necessário adicionar gateways e tabelas de rotas.

Considerações

- Você deve especificar um bloco CIDR IPv4 para a sub-rede a partir do intervalo da sua VPC. Como opção, você poderá especificar um bloco CIDR IPv6 para sua sub-rede se houver um bloco CIDR IPv6 associado à VPC. Para ter mais informações, consulte Endereçamento IP para suas VPCs e sub-redes.
- Se você criar uma sub-rede exclusivamente IPv6, esteja ciente do seguinte: Uma instância do EC2 iniciada em uma sub-rede exclusivamente IPv6 recebe um endereço IPv6, mas não um endereço IPv4. Qualquer instância que você inicie em uma sub-rede exclusivamente IPv6 precisa ser uma instância criada no Nitro System.
- Para criar a sub-rede em uma zona local ou zona Wavelength, é necessário habilitar a zona. Para obter mais informações, consulte Regiões e zonas no Guia do usuário do Amazon EC2.

Adicionar uma sub-rede à VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Sub-redes.
3. Escolha Criar sub-rede.
4. Em ID da PC escolha a VPC para a sub-rede.
5. (Opcional) Em Subnet name (Nome da sub-rede), insira um nome para a sub-rede. Ao fazer isso, é criada uma tag com a chave `Name` e o valor especificado.
6. Em Availability Zone (Zona de disponibilidade), é possível escolher uma zona para a sub-rede ou deixar a opção padrão No Preference (Sem preferência) para que a AWS escolha uma para você.
7. Para o bloco de CIDR IPv4, selecione Entrada manual para inserir um bloco IPv4 CIDR para sua sub-rede (por exemplo, `10.0.1.0/24`) ou selecione Sem CIDR IPv4. Se estiver usando o IP Address Manager (IPAM) do Amazon VPC para planejar, rastrear e monitorar endereços IP para suas workloads de AWS, ao criar uma sub-rede, você terá a opção de alocar um bloco CIDR do IPAM (alocado pelo IPAM). Para obter mais informações sobre como planejar o espaço de endereço IP da VPC para alocações de IP de sub-rede, consulte Tutorial: Planejar o espaço de endereço IP da VPC para alocações de IP de sub-rede no Guia do usuário do IPAM do Amazon VPC .
8. Para o bloco IPv6 CIDR, selecione Entrada manual para escolher o CIDR da VPC IPv6 em que você deseja criar uma sub-rede. Essa opção só fica disponível se a VPC tiver um bloco CIDR IPv6 associado. Se estiver usando o IP Address Manager (IPAM) do Amazon VPC para

planejar, rastrear e monitorar endereços IP para suas workloads de AWS, ao criar uma sub-rede, você terá a opção de alocar um bloco CIDR do IPAM (alocado pelo IPAM). Para obter mais informações sobre como planejar o espaço de endereço IP da VPC para alocações de IP de sub-rede, consulte Tutorial: Planejar o espaço de endereço IP da VPC para alocações de IP de sub-rede no Guia do usuário do IPAM do Amazon VPC .

9. Escolha um bloco CIDR da VPC IPv6.
10. Para o bloco CIDR de sub-rede IPv6, escolha um CIDR para a sub-rede que seja igual ou mais específico que o CIDR da VPC. Por exemplo, se o CIDR do grupo da VPC for /50, você poderá escolher um comprimento de máscara de rede entre /50 e /64 para a sub-rede. Os possíveis comprimentos de máscara de rede IPv6 estão entre /44 e /64 em incrementos de /4.
11. Escolha Criar sub-rede.

Para adicionar uma sub-rede à sua VPC usando a AWS CLI

Use o comando create-subnet.

Próximas etapas

Após criar uma sub-rede, você poderá configurá-la da seguinte maneira:

- Configure o roteamento. Em seguida, você pode criar uma tabela de rotas personalizada e encaminhar esse tráfego para um gateway associado à VPC, como um gateway da Internet. Para ter mais informações, consulte Configurar tabelas de rotas.
- Modifique o comportamento do endereçamento IP. É possível especificar se as instâncias iniciadas na sub-rede recebem um endereço IPv4 público, um endereço IPv6 ou ambos. Para ter mais informações, consulte Modificar os atributos de endereçamento IP da sua sub-rede.
- Modifique as configurações de Resource-based Name (RBN – Nome baseado em recurso). Para obter mais informações, consulte Tipos de nomes do host de instâncias do Amazon EC2.
- Crie ou modifique suas ACLs de rede. Para ter mais informações, consulte Controlar o tráfego da sub-rede com listas de controle de acesso à rede.
- Compartilhe a sub-rede com outras contas. Para ter mais informações, consulte ???.

Adicionar ou remover um bloco CIDR IPv6 da sua sub-rede

Você pode associar um bloco CIDR IPv6 a uma sub-rede existente na sua VPC. A sub-rede não deve ter um bloco CIDR IPv6 existente associado a ela.

Se não você não desejar mais compatibilidade com IPv6 em sua sub-rede, mas quiser continuar usando sua sub-rede para criar e se comunicar com recursos IPv4, o bloco CIDR IPv6 poderá ser removido.

Antes de poder remover um bloco CIDR IPv6, primeiro é necessário cancelar a atribuição de quaisquer endereços IPv6 atribuídos a qualquer instância em sua sub-rede.

Para adicionar ou remover um bloco CIDR IPv6 de uma sub-rede

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Sub-redes.
3. Selecione sua sub-rede e escolha Actions (Ações), Edit CIDRs IPv6 (Editar CIDRs IPv6).
4. Para adicionar um CIDR, escolha Adicionar CIDR IPv6, escolha um Bloco CIDR da VPC, insira um Bloco CIDR da sub-rede e escolha um comprimento de máscara de rede igual ou mais específico do que o comprimento da máscara de rede do CIDR da VPC. Por exemplo, se o CIDR do grupo da VPC for /50, você poderá escolher um comprimento de máscara de rede entre /50 e /64 para a sub-rede. Os possíveis comprimentos de máscara de rede IPv6 estão entre /44 e /64 em incrementos de /4.
5. Para remover um CIDR, localize o bloco CIDR IPv6 e escolha Remover.
6. Escolha Salvar.

Para associar um bloco CIDR IPv6 a uma sub-rede usando a AWS CLI

Use o comando associate-subnet-cidr-block.

Para desassociar um bloco CIDR IPv6 de uma sub-rede usando a AWS CLI

Use o comando disassociate-subnet-cidr-block.

Modificar os atributos de endereçamento IP da sua sub-rede

Por padrão, as sub-redes não padrão apresentam o atributo de endereçamento público IPv4 configurado como `false` e as sub-redes padrão têm esse atributo definido como `true`. Uma exceção é uma sub-rede não padrão criada pelo assistente de instância de inicialização do Amazon EC2: o assistente define o atributo como `true`. É possível modificar este atributo usando o console da Amazon VPC.

Por padrão, todas as sub-redes possuem o atributo de endereçamento IPv6 configurado como `false`. É possível modificar este atributo usando o console da Amazon VPC. Se você habilitar o atributo de endereçamento IPv6 para sua sub-rede, as interfaces de rede criadas na sub-rede recebem um endereço IPv6 do intervalo da sub-rede. As instâncias iniciadas na sub-rede recebem um endereço IPv6 na interface de rede primária.

Sua sub-rede deve ter um bloco CIDR IPv6 associado.

> **Note**
>
> Se você habilitar o recurso de endereçamento IPv6 para a sua sub-rede, sua interface de rede ou instância só receberá um endereço IPv6 se for criado usando a versão `2016-11-15` ou superior da API do Amazon EC2. O console do Amazon EC2 usa a versão mais recente da API.

Para modificar o comportamento de endereçamento da sub-rede

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Sub-redes.
3. Selecione a sua sub-rede e escolha Actions (Ações) e Edit subnet settings (Editar configurações de sub-redes).
4. A caixa de seleção Ativar a atribuição automática de endereço IPv4 público, se selecionada, solicita um endereço IPv4 público para todas as instâncias iniciadas na sub-rede selecionada. Marque ou desmarque a caixa de seleção conforme necessário, e selecione Save.
5. A caixa de seleção Habilitar a atribuição automática de endereço IPv6, se selecionada, solicita um endereço IPv6 para todas as interfaces de rede criadas na sub-rede selecionada. Marque ou desmarque a caixa de seleção conforme necessário, e selecione Save.

Para modificar um atributo de sub-rede usando a AWS CLI

Use o comando modify-subnet-attribute.

Reservas do CIDR da sub-rede

Uma reserva CIDR de sub-rede é um intervalo de endereços IPv4 ou IPv6 que você reserva para que a AWS não os atribua às interfaces de rede. Isso permite que você reserve blocos CIDR IPv4 ou IPv6 (também chamados de “prefixos”) para uso com as interfaces de rede.

Ao criar uma reserva CIDR de sub-rede, você especifica como usará os endereços IP reservados. As seguintes opções estão disponíveis:

- Prefixo: permite atribuir um prefixo a uma única interface de rede. Para obter mais informações, consulte Atribuir prefixos a interfaces de rede do Amazon EC2 no Guia do usuário do Amazon EC2.
- Explícito: permite atribuir manualmente um endereço IP individual a uma única interface de rede.

As seguintes regras se aplicam às reservas CIDR de sub-rede:

- Quando você cria uma reserva CIDR de sub-rede, o intervalo de endereços IP pode incluir endereços que já estão em uso. Criar uma reserva de sub-rede não cancela a atribuição de nenhum endereço IP que já esteja em uso.
- É possível reservar vários intervalos de CIDR por sub-rede. Quando você reserva vários intervalos de CIDR dentro da mesma VPC, os intervalos de CIDR não podem se sobrepor.
- Quando você reserva mais de um intervalo em uma sub-rede para delegação de prefixo e a delegação de prefixo está configurada para atribuição automática, os endereço IP são escolhidos para serem atribuídos à interface de rede aleatoriamente.
- Quando você exclui uma reserva de sub-rede, os endereços IP não utilizados ficam disponíveis para a AWS atribuir às interfaces de rede. Excluir uma reserva de sub-rede não cancela a atribuição de nenhum endereço IP que já esteja em uso.

Para obter mais informações sobre a notação Encaminhamento Entre Domínios Sem Classificação (CIDR), consulte Endereçamento IP.

Conteúdo

Trabalhar com reservas de CIDR de sub-rede usando o console

É possível criar e gerenciar reservas de CIDR de sub-rede conforme mostrado a seguir.

Para editar reservas de CIDR de sub-rede

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Sub-redes.
3. Selecione a sub-rede.
4. Escolha a guia Reservas de CIDR para obter informações sobre qualquer reserva de CIDR de sub-rede existente.
5. Para adicionar ou remover reservas de CIDR de sub-redes, escolha Ações, Editar reservas de CIDR e faça o seguinte:
   - Para adicionar uma reserva do CIDR do IPv4, escolha IPv4, Add IPv4 CIDR reservation (Adicionar reserva do CIDR do IPv4). Escolha o tipo de reserva, insira o intervalo do CIDR e escolha Add (Adicionar).
   - Para adicionar uma reserva do CIDR do IPv6, escolha IPv6, Add IPv6 CIDR reservation (Adicionar reserva do CIDR do IPv6). Escolha o tipo de reserva, insira o intervalo do CIDR e escolha Add (Adicionar).
   - Para remover uma reserva de CIDR, escolha Remover para a reserva CIDR de sub-rede.

Trabalhar com reservas de CIDR de sub-rede usando a AWS CLI

É possível usar o AWS CLI para criar e gerenciar reservas de CIDR de sub-rede.

Tarefas

- Criar uma reserva CIDR de sub-rede
- Ver reservas de sub-rede CIDR
- Excluir uma reserva CIDR de sub-rede

Criar uma reserva CIDR de sub-rede

É possível usar o create-subnet-cidr-reservation para criar uma reserva CIDR de sub-rede.

```
aws ec2 create-subnet-cidr-reservation --subnet-id subnet-03c51e2eEXAMPLE --
reservation-type prefix --cidr 2600:1f13:925:d240:3a1b::/80
```

O seguinte é um exemplo de saída.

```
{
    "SubnetCidrReservation": {
        "SubnetCidrReservationId": "scr-044f977c4eEXAMPLE",
        "SubnetId": "subnet-03c51e2ef5EXAMPLE",
        "Cidr": "2600:1f13:925:d240:3a1b::/80",
        "ReservationType": "prefix",
        "OwnerId": "123456789012"
    }
}
```

Ver reservas de sub-rede CIDR

É possível usar o get-subnet-cidr-reservations para ver os detalhes de uma reserva CIDR da sub-rede.

```
aws ec2 get-subnet-cidr-reservations --subnet-id subnet-05eef9fb78EXAMPLE
```

Excluir uma reserva CIDR de sub-rede

É possível usar o delete-subnet-cidr-reservation para excluir uma reserva CIDR de sub-rede.

```
aws ec2 delete-subnet-cidr-reservation --subnet-cidr-reservation-
id scr-044f977c4eEXAMPLE
```

Configurar tabelas de rotas

Uma tabela de rotas contém um conjunto de regras, chamado de rotas, que determinam para onde o tráfego de rede de sua sub-rede ou gateway é direcionado.

Conteúdo

- Conceitos da tabela de rotas
- Tabelas de rotas de sub-rede

- Tabelas de rotas do gateway
- Prioridade de rota
- Exemplo de opções de roteamento
- Alterar a tabela de rotas de uma sub-rede
- Substituir a tabela de rotas principal
- Controle o tráfego que entra na sua VPC com uma tabela de rotas de gateway
- Substituir ou restaurar o destino de uma rota local
- Solucionar problemas de acessibilidade

Conceitos da tabela de rotas

Os conceitos principais das tabelas de rotas são os seguintes.

- Tabela de rotas principal: a tabela de rotas que vem automaticamente com a VPC. Ela controla o roteamento de todas as sub-redes que não estejam explicitamente associadas com outra tabela de rotas.
- Tabela de rotas personalizada: uma tabela de rotas criada para a VPC.
- Destination (Destino): o intervalo de endereços IP para onde você deseja que o tráfego vá (CIDR de destino). Por exemplo, uma rede corporativa externa com um CIDR `172.16.0.0/12`.
- Target (Destino): o gateway, a interface de rede ou a conexão por meio da qual enviar o tráfego de destino, por exemplo, um gateway da Internet.
- Route table association (Associação de tabelas de rotas): a associação entre uma tabela de rotas e uma sub-rede, gateway da Internet ou gateway privado virtual.
- Subnet route table (Tabela de rotas de sub-rede): uma tabela de rotas associada a uma sub-rede.
- Local route (Rota local): uma rota padrão para comunicação dentro da VPC.
- Propagação: se você tiver anexado um gateway privado virtual à sua VPC e habilitado a propagação de rotas, adicionaremos automaticamente rotas para a conexão da sua VPN com suas tabelas de rotas de sub-rede. Isso significa que você não precisará adicionar ou remover rotas VPN manualmente. Para mais informações, consulte Opções de roteamento do Site-to-Site VPN no Guia do usuário do Site-to-Site VPN.
- Tabela de rotas de gateway: uma tabela de rotas associada a um gateway da Internet ou gateway privado virtual.

- Associação de borda : uma tabela de rotas usada para encaminhar o tráfego de entrada da VPC para um dispositivo. Associe uma tabela de rotas ao gateway da Internet ou ao gateway privado virtual e especifique a interface de rede do seu equipamento como destino do tráfego da VPC.
- Tabela de rotas de gateway de trânsito: uma tabela de rotas associada a um gateway de trânsito. Para obter mais informações, consulte Tabelas de rota de Transit gateway em Amazon VPC Transit Gateway.
- Tabela de rotas de gateway local: uma tabela de rotas associada a um gateway local do Outposts. Para obter mais informações, consulte Gateways locais no Guia do usuário do AWS Outposts.

Tabelas de rotas de sub-rede

Sua VPC tem um roteador implícito e você usa tabelas de rotas para controlar para onde o tráfego de rede é direcionado. Toda sub-rede em sua VPC deve ser associada a uma tabela de rotas, que controla o roteamento para a sub-rede (tabela de rotas de sub-rede). Você pode associar explicitamente uma sub-rede a uma tabela de rotas específica. Caso contrário, a sub-rede é implicitamente associada à tabela de rotas principal. Uma sub-rede só pode ser associada a uma única tabela de rotas por vez, mas é possível associar várias sub-redes a uma mesma tabela de rotas de sub-rede.

Conteúdo

Rotas

Cada rota em uma tabela especifica um destino e um alvo. Por exemplo, para permitir que a sub-rede acesse a Internet por meio de um gateway da Internet, adicione a seguinte rota à tabela de rotas de sub-rede. O destino da rota é `0.0.0.0/0`, que representa todos os endereços IPv4. O alvo é o gateway da Internet que está conectado à sua VPC.

Destino	Destino
0.0.0.0/0	*igw-id*

Os blocos CIDR para IPv4 e IPv6 são tratados separadamente. Por exemplo, uma rota com um CIDR de destino de `0.0.0.0/0` não inclui automaticamente todos os endereços IPv6. Você precisa criar uma rota com um CIDR de destino de `::/0` para todos os endereços IPv6.

Se você faz com frequência referência ao mesmo conjunto de blocos CIDR nos recursos da AWS, poderá criar uma lista de prefixos gerenciados pelo cliente para agrupá-los. Depois, você pode especificar a lista de prefixos como destino na entrada da tabela de rotas.

Toda tabela de rotas contém uma rota local para comunicação dentro da VPC. Esta rota é adicionada por padrão a todas as tabelas de rotas. Se a VPC tiver mais de um bloco CIDR IPv4, as tabelas de rotas conterão um rota local para cada bloco CIDR IPv4. Se tiver associado um bloco CIDR IPv6 à VPC, as tabelas de rotas conterão uma rota local para o bloco CIDR IPv6. É possível substituir ou restaurar o destino de cada uma das rotas locais conforme necessário.

Regras e considerações

- Você pode adicionar uma rota às suas tabelas de rotas que seja mais específica do que a rota local. O desino deve corresponder a todo o bloco CIDR IPv4 ou IPv6 de uma sub-rede em sua VPC. O destino deve ser um gateway NAT, uma interface de rede ou um endpoint de balanceador de carga de gateway.
- Se sua tabela de rotas tiver várias rotas, usamos a rota mais específica que corresponde ao tráfego (correspondência de prefixo mais longa) para determinar como rotear o tráfego.
- Não é possível adicionar rotas a endereços IPv4 que sejam uma correspondência exata ou um subconjunto do seguinte intervalo: 169.254.168.0/22. Esse intervalo está no espaço de endereço local do link e é reservado para uso por serviços da AWS. Por exemplo, o Amazon EC2 usa endereços nesse intervalo para serviços que são acessíveis exclusivamente de instâncias do EC2, como o Instance Metadata Service (IMDS) e o servidor de DNS da Amazon. Você pode usar um bloco CIDR que seja maior que, mas se sobreponha a 169.254.168.0/22, mas os pacotes destinados a endereços no intervalo 169.254.168.0/22 não serão encaminhados.
- Não é possível adicionar rotas a endereços IPv6 que sejam uma correspondência exata ou um subconjunto do seguinte intervalo: fd00:ec2::/32. Esse intervalo está no espaço de Unique Local Address (ULA – Endereço local exclusivo) e é reservado para uso por serviços da AWS. Por exemplo, o Amazon EC2 usa endereços nesse intervalo para serviços que são acessíveis exclusivamente de instâncias do EC2, como o Instance Metadata Service (IMDS) e o servidor de DNS da Amazon. Você pode usar um bloco CIDR que seja maior que, mas se sobreponha a fd00:ec2::/32, mas os pacotes destinados a endereços no intervalo fd00:ec2::/32 não serão encaminhados.

- Você pode adicionar dispositivos middlebox aos caminhos de roteamento para a sua VPC. Para ter mais informações, consulte the section called “Roteamento para um dispositivo Middlebox”.

Exemplo

No exemplo a seguir, suponha que uma VPC tem um bloco CIDR IPv4 e um bloco CIDR IPv6. Os tráfegos IPv4 e IPv6 são tratados separadamente, conforme mostrado na tabela de rotas a seguir.

Destino	Destino
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Local
172.31.0.0/16	pcx-11223344556677889
0.0.0.0/0	igw-12345678901234567
::/0	eigw-aabbccddee1122334

- O tráfego IPv4 a ser roteado dentro da VPC (10.0.0.0/16) é abrangido pela rota Local.
- O tráfego IPv6 a ser roteado dentro da VPC (2001:db8:1234:1a00::/56) é abrangido pela rota Local.
- A rota para 172.31.0.0/16 envia o tráfego para uma conexão de emparelhamento.
- A rota para todo o tráfego IPv4 (0.0.0.0/0) envia o tráfego para um gateway da Internet. Portanto, todo o tráfego IPv4, exceto o tráfego dentro da VPC e para a conexão de emparelhamento, é roteado para o gateway da Internet.
- A rota para todo o tráfego IPv6 (::/0) envia o tráfego para um gateway da Internet somente de saída. Portanto, todo o tráfego IPv6, exceto o tráfego dentro da VPC, é roteado para o gateway da Internet somente de saída.

Tabela de rotas principal

Quando você cria uma VPC, a tabela de rotas principal é criada automaticamente. Quando uma sub-rede não tem uma tabela de roteamento explicitamente associada, ela usará a tabela de roteamento

principal por padrão. Para visualizar a tabela de rotas principal de uma VPC, na página Route Tables (Tabelas de rotas), no console da Amazon VPC, procure por Yes (Sim) na coluna Main (Principal).

Por padrão, quando você cria uma VPC não padrão, a tabela de rotas principal contém apenas uma rota local. Se você Crie uma VPC e escolher um gateway NAT, a Amazon VPC adicionará rotas automaticamente à tabela de rotas principal para os gateways.

As seguintes regras se aplicam à tabela de rotas principal:

- Você pode adicionar, remover e modificar rotas na tabela de rotas principal.
- Você não pode excluir a tabela de rotas principal.
- Você não pode definir uma tabela de rotas de gateway como a tabela de rotas principal.
- Você pode substituir a tabela de rotas principal ao associar uma tabela de rotas personalizada a uma sub-rede.
- Você pode associar explicitamente uma sub-rede à tabela de rotas principal, mesmo que ela já esteja implicitamente associada.

  Você pode querer fazer isso se alterar qual tabela é a tabela de rotas principal. Quando você altera a tabela que constitui a tabela de rotas principal, isso também altera o padrão para novas sub-redes ou para sub-redes que não estejam explicitamente associadas a outra tabela de rotas. Para obter mais informações, consulte Substituir a tabela de rotas principal.

Tabelas de rotas personalizadas

Por padrão, uma tabela de rotas contém uma rota local para comunicação na VPC. Se você Crie uma VPC e escolher uma sub-rede pública, a Amazon VPC criará uma tabela de rotas personalizada e adicionará uma rota que aponte para o gateway da Internet. Uma maneira de proteger sua VPC é deixar a tabela de rotas principal em seu estado padrão original. Depois, associe explicitamente cada nova sub-rede criada a uma das tabelas de rotas personalizadas criadas. Desse modo, você pode controlar explicitamente como cada sub-rede roteia o tráfego.

Você pode adicionar, remover e modificar rotas em uma tabela de rotas personalizada. Você poderá excluir uma tabela de rotas personalizada somente se ela não tiver associações.

Associação da tabela de rotas da sub-rede

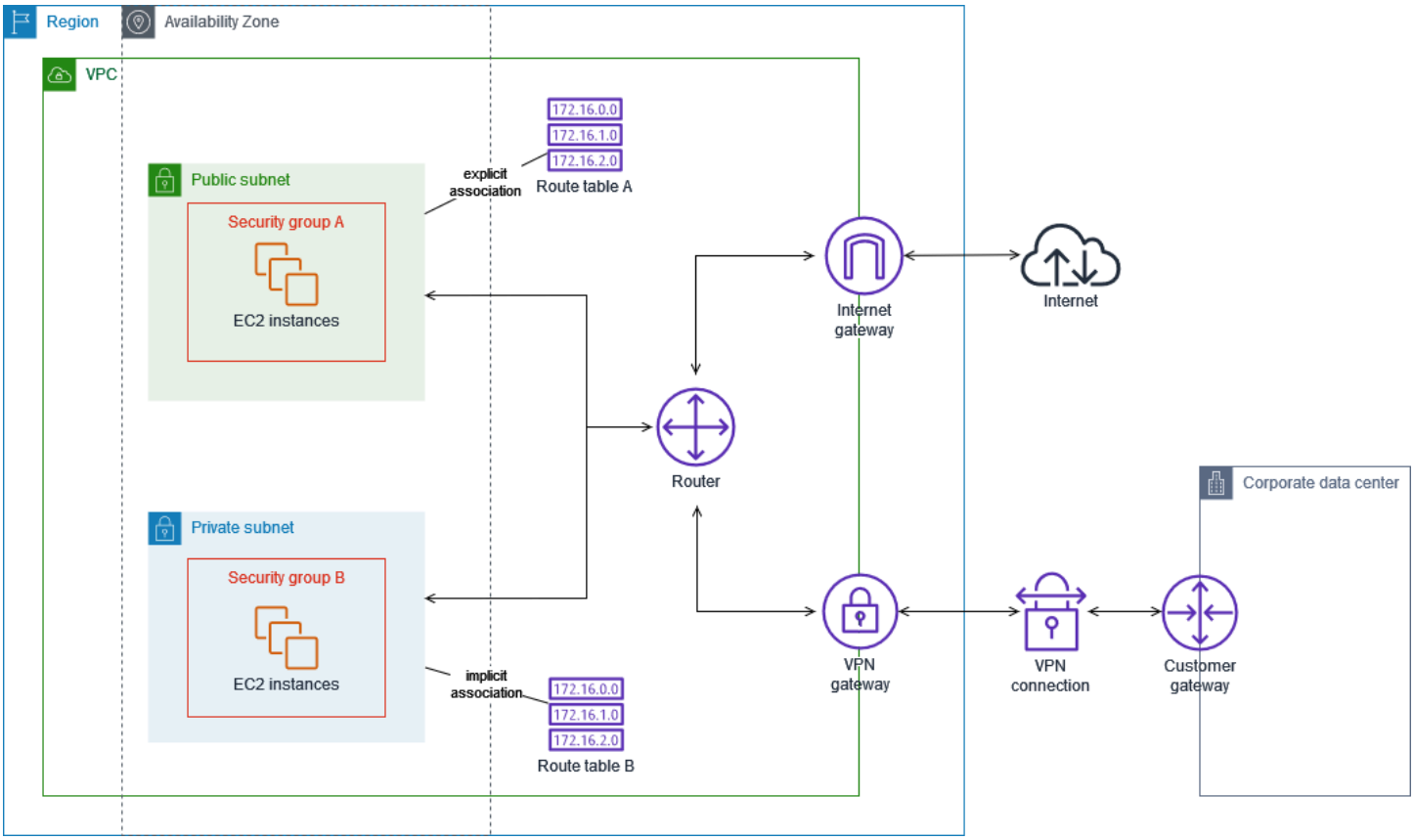
Toda sub-rede em sua VPC deve ser associada a uma tabela de rotas. Uma sub-rede pode ser explicitamente associada à tabela de rotas personalizada, ou implicitamente ou explicitamente

associada à tabela de rotas principal. Para obter mais informações sobre como visualizar suas associações de sub-rede e tabela de rotas, consulte Determinar as sub-redes e/ou os gateways explicitamente associadas.

As sub-redes que estão em VPCs associadas ao Outposts podem ter um tipo de destino adicional de um gateway local. Essa é a única diferença de roteamento das sub-redes que não são de Outposts.

Exemplo 1: Associação de sub-rede implícita e explícita

O diagrama a seguir mostra o roteamento para uma VPC com um gateway da Internet, um gateway privado virtual, uma sub-rede pública e uma sub-rede somente VPN.



A tabela de rotas A é uma tabela de rotas personalizada que está explicitamente associada à sub-rede pública. Ela tem uma rota que envia todo o tráfego para o gateway da Internet, que é o que torna a sub-rede uma sub-rede pública.

Destino	Alvo
CIDR DA VPC	Local

Destino	Alvo
0.0.0.0/0	*igw-id*

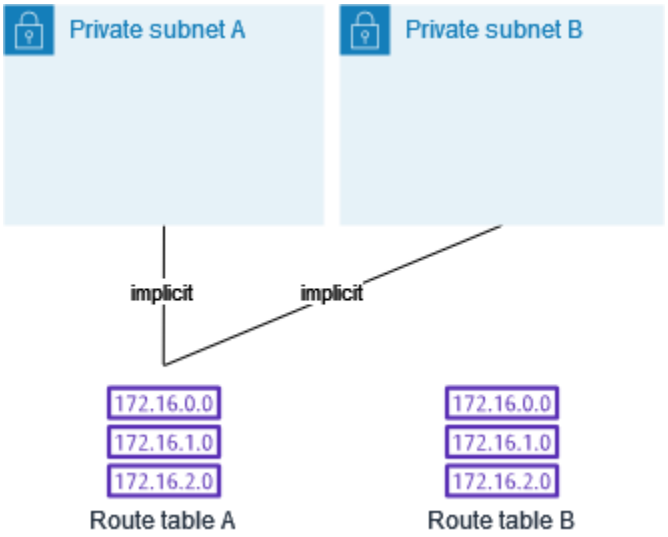
A tabela de rotas B é a tabela de rotas principal. Ela está implicitamente associada à sub-rede privada. Ela tem uma rota que envia todo o tráfego para o gateway privado virtual, mas nenhuma rota para o gateway da Internet, que é o que torna a sub-rede uma sub-rede somente para VPN. Se você criar outra sub-rede nesta VPC e não associar uma tabela de rotas personalizada, a sub-rede também será associada implicitamente a esta tabela de rotas porque é a tabela de rotas principal.

Destino	Alvo
CIDR DA VPC	Local
0.0.0.0/0	*vgw-id*

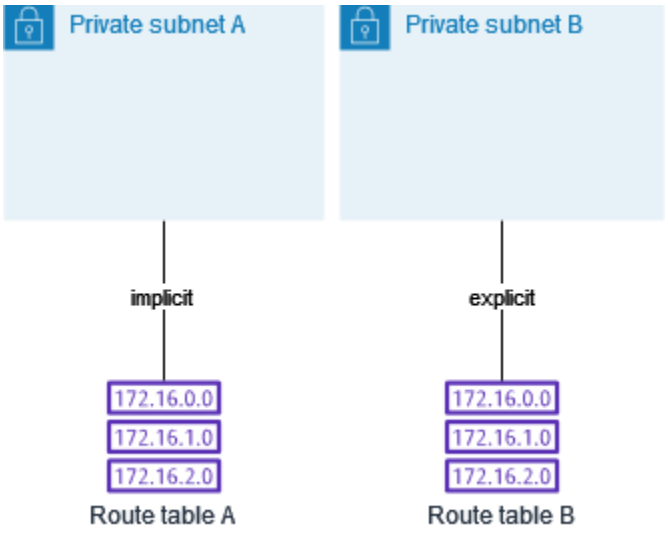
Exemplo 2: Substituir a tabela de rotas principal

Você pode querer fazer alterações na tabela de rotas principal. Para evitar qualquer interrupção no tráfego, recomendamos que você primeiro teste as alterações de rota usando uma tabela de rotas personalizada. Quando estiver satisfeito com o teste, você pode substituir a tabela de rotas principal pela nova tabela personalizada.

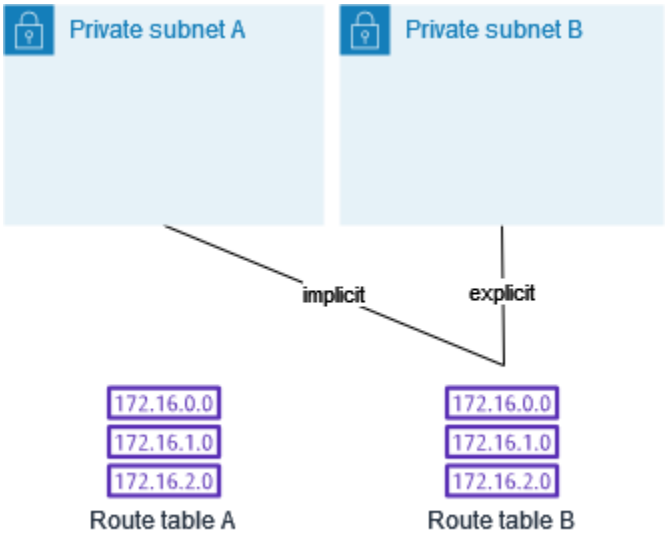
O diagrama a seguir mostra duas sub-redes e duas tabelas de rotas. A sub-rede A está implicitamente associada à tabela de rotas A, a tabela de rotas principal. A sub-rede B está implicitamente associada à tabela de rotas A. A tabela de rotas B, uma tabela de rotas personalizada, não está associada a nenhuma sub-rede.



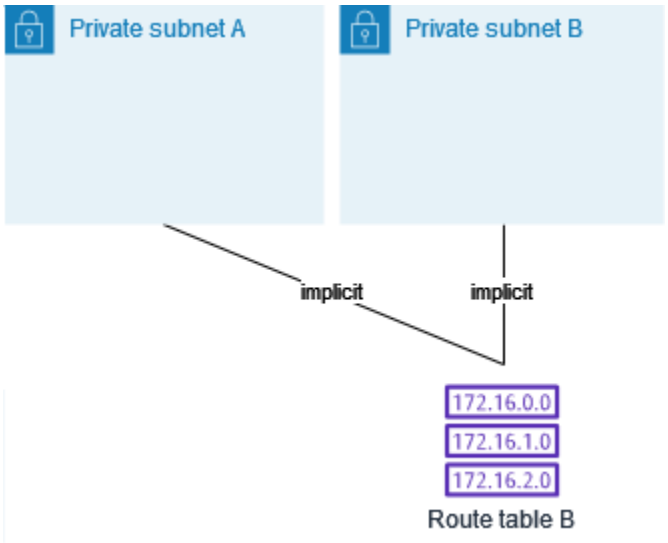
Para substituir a tabela de rotas principal, comece criando uma associação explícita entre a sub-rede B e a tabela de rotas B. Teste a tabela de rotas B.



Depois de testar a tabela de rotas B, torne-a a tabela de rotas principal. A sub-rede B ainda tem uma associação explícita com a tabela de rotas B. No entanto, a sub-rede A passou a ter uma associação implícita com a tabela de rotas B, pois a tabela de rotas B é a nova tabela de rotas principal. A tabela de rotas A não está mais associada a nenhuma sub-rede.



(Opcional) Se você desassociar a sub-rede B da tabela de rotas B, ainda haverá uma associação implícita entre a sub-rede B e a tabela de rotas B. Se você não precisar mais da tabela de rotas A, poderá excluí-la.



Tabelas de rotas do gateway

Você pode associar uma tabela de rotas a um gateway da Internet ou a um gateway privado virtual. Quando uma tabela de rotas é associada a um gateway, ela é chamada de tabela de rotas de gateway. Você pode criar uma tabela de rotas de gateway para controle detalhado do caminho de roteamento do tráfego que entra na VPC. Por exemplo, é possível interceptar o tráfego que entra na VPC por meio de um gateway da Internet redirecionando esse tráfego para um dispositivo Middlebox (por exemplo, um dispositivo de segurança) na VPC.

Conteúdo

Rotas da tabelas de rotas do gateway

Uma tabela de rotas de gateway associada a um gateway da Internet oferece suporte a rotas com os seguintes destinos:

- A rota local padrão
- Um endpoint do balanceador de carga do gateway
- Uma interface de rede para um dispositivo middlebox

Uma tabela de rotas de gateway associada a um gateway privado virtual oferece suporte a rotas com os seguintes destinos:

- A rota local padrão
- Um endpoint do balanceador de carga do gateway
- Uma interface de rede para um dispositivo middlebox

Quando o destino for um endpoint do Gateway Load Balancer ou uma interface de rede, os seguintes destinos são permitidos:

- Todo o bloco CIDR IPv4 ou IPv6 da sua VPC. Nesse caso, você substitui o alvo da rota local padrão.
- Todo o bloco CIDR IPv4 ou IPv6 de uma sub-rede em sua VPC. Esta é uma rota mais específica do que a rota local padrão.

Se você alterar o alvo da rota local em uma tabela de rotas de gateway para uma interface de rede em sua VPC, poderá restaurá-la posteriormente para o alvo padrão `local`. Para ter mais informações, consulte Substituir ou restaurar o destino de uma rota local.

Exemplo

Na tabela de rotas de gateway a seguir, o tráfego destinado a uma sub-rede com o bloco CIDR `172.31.0.0/20` é roteado para uma interface de rede específica. O tráfego destinado a todas as outras sub-redes na VPC usa a rota local.

Destino	Destino
172.31.0.0/16	Local
172.31.0.0/20	*eni-id*

Exemplo

Na tabela de rotas de gateway a seguir, o alvo da rota local é substituído por um ID de interface de rede. O tráfego destinado a todas as sub-redes dentro da VPC é roteado para a interface de rede.

Destino	Destino
172.31.0.0/16	*eni-id*

Regras e considerações

Não será possível associar uma tabela de rotas a um gateway se qualquer uma das seguintes afirmações se aplicar:

- A tabela de rotas contém rotas existentes com destinos diferentes de uma interface de rede, endpoint do Gateway Load Balancer ou da rota local padrão.
- A tabela de rotas contém rotas existentes para blocos CIDR fora dos intervalos em sua VPC.
- A propagação de rota está ativada para a tabela de rotas.

Além disso, as seguintes regras e considerações são aplicáveis:

- Não é possível adicionar rotas a nenhum bloco CIDR fora dos intervalos em sua VPC, incluindo intervalos maiores que os blocos CIDR individuais da VPC.
- Você só pode especificar `local`, um endpoint do Gateway Load Balancer ou uma interface de rede como destino. Não é possível especificar outros tipos de destinos, incluindo endereços IP de

host individuais. Para ter mais informações, consulte the section called “Exemplo de opções de roteamento”.

- Não é possível especificar uma lista de prefixos como destino.
- Não é possível usar uma tabela de rotas de gateway para controlar ou interceptar tráfego fora da VPC, como o tráfego por meio de um gateway de trânsito conectado, por exemplo. Você pode interceptar o tráfego que entra na VPC e redirecioná-lo para outro alvo somente na mesma VPC.
- Para garantir que o tráfego atinja o dispositivo Middlebox, a interface de rede de destino deve ser associada a uma instância em execução. Para tráfego que flui por um gateway da Internet, a interface de rede de destino também deve ter um endereço IP público.
- Ao configurar seu dispositivo Middlebox, tome nota das considerações sobre o dispositivo.
- Quando você roteia o tráfego por meio de um dispositivo Middlebox, o tráfego de retorno da sub-rede de destino deve ser roteado pelo mesmo dispositivo. Não há suporte ao roteamento assimétrico.
- As regras da tabela de rotas aplicam-se a todo o tráfego que sai de uma sub-rede. O tráfego que sai de uma sub-rede é definido como tráfego destinado ao endereço MAC do roteador de gateway dessa sub-rede. O tráfego destinado ao endereço MAC de outra interface de rede nessa sub-rede faz uso do roteamento de enlace de dados (camada 2) em vez de rede (camada 3). Por isso, as regras não se aplicam a esse tráfego.
- Nem todas as Zonas Locais oferecem suporte à associação de borda com gateways privados virtuais. Para obter mais informações sobre as zonas disponíveis, consulte Considerações no Guia do Usuário de Zonas Locais da AWS .

Prioridade de rota

Em geral, direcionamos o tráfego usando a rota mais específica correspondente ao tráfego. Isso é conhecido como a correspondência de prefixo mais longa. Se a tabela de rotas tiver rotas sobrepostas ou correspondentes, serão aplicadas regras adicionais.

A lista a seguir mostra um resumo da prioridade da rota com links para as seções abaixo com informações e exemplos mais detalhados:

1. Prefixo mais longo (por exemplo, 10.10.2.15/32 tem prioridade sobre 10.10.2.0/24)
2. Rotas estáticas (como emparelhamento de VPC e conexões de gateway da internet)
3. Rotas da lista de prefixos
4. Rotas propagadas

a. Rotas do BGP do Direct Connect (rotas dinâmicas)
b. Rotas estáticas da VPN
c. Rotas do BGP da VPN (rotas dinâmicas) (como gateways privados virtuais)

A correspondência de prefixo mais longa

As rotas para endereços IPv4 e IPv6 ou blocos CIDR são independentes umas das outras. Usamos a rota mais específica que corresponde ao tráfego IPv4 ou ao tráfego IPv6 para determinar como rotear o tráfego.

O exemplo de tabela de rotas de sub-rede a seguir tem uma rota para o tráfego de Internet IPv4 (`0.0.0.0/0`) direcionada para um gateway da Internet e uma rota para o tráfego IPv4 `172.31.0.0/16` direcionada para uma conexão de emparelhamento (`pcx-11223344556677889`). Qualquer tráfego da sub-rede destinado ao intervalo de endereços IP `172.31.0.0/16` usa a conexão de emparelhamento, porque essa rota é mais específica do que a rota para o gateway da Internet. Qualquer tráfego que vá para um alvo dentro da VPC (`10.0.0.0/16`) é coberto pela rota `local` e, portanto, roteado dentro da VPC. Todos os outros tráfegos da sub-rede usam o gateway da Internet.

Destino	Destino
10.0.0.0/16	local
172.31.0.0/16	pcx-11223344556677889
0.0.0.0/0	igw-12345678901234567

Prioridade de rota para rotas estáticas e propagadas dinamicamente

Se você tiver anexado um gateway privado virtual à sua VPC e habilitado a propagação de rotas em sua tabela de rotas de sub-rede, as rotas que representam a conexão do Site-to-Site VPN aparecerão automaticamente na tabela de rotas como rotas propagadas.

Se o destino de uma rota propagada for idêntico ao destino de uma rota estática, a rota estática terá prioridade. Os seguintes recursos usam rotas estáticas:

- internet gateway (gateway da Internet)

- nat gateway
- Interface de rede
- ID da instância
- VPC endpoint de gateway
- Transit gateway
- Conexão de emparelhamento de VPC
- Endpoint do Gateway Load Balancer

Para obter mais informações, consulte Tabelas de rotas e prioridade de rotas da VPN no Manual do usuário da AWS Site-to-Site VPN.

O exemplo de tabela de rotas a seguir tem uma rota estática para um gateway da Internet e uma rota propagada para um gateway privado virtual. O destino de ambas as rotas é `172.31.0.0/24`. Como uma rota estática para um gateway da Internet tem prioridade, todo o tráfego destinado para `172.31.0.0/24` é roteado para o gateway da internet.

Destino	Alvo	Com propagação
10.0.0.0/16	local	Não
172.31.0.0/24	vgw-11223344556677889	Sim
172.31.0.0/24	igw-12345678901234567	Não

Prioridade de rotas para listas de prefixos

Se a tabela de rotas fizer referência a uma lista de prefixos, as seguintes regras serão aplicadas:

- Se a tabela de rotas contiver uma rota estática com um bloco CIDR de destino que se sobreponha a uma rota estática com uma lista de prefixos, a rota estática com o bloco CIDR terá prioridade.
- Se a tabela de rotas contiver uma rota propagada que corresponde a uma rota que faz referência a uma lista de prefixos, a rota que faz referência à lista de prefixos terá prioridade. No caso de rotas que se sobrepõem, rotas mais específicas sempre têm prioridade, independentemente do fato de serem propagadas, estáticas ou que fazem referência a listas de prefixos.

- Se sua tabela de rotas fizer referência a várias listas de prefixos que têm blocos CIDR sobrepostos para destinos diferentes, escolheremos aleatoriamente qual rota terá prioridade. Depois disso, a mesma rota terá prioridade sempre.

Exemplo de opções de roteamento

Os tópicos a seguir descrevem o roteamento para gateways específicos ou conexões em sua VPC.

Conteúdo

Roteamento para um gateway da Internet

Você pode tornar uma sub-rede pública adicionando uma rota em sua tabela de rotas de sub-rede a um gateway da Internet. Para isso, crie e anexe um gateway da Internet à sua VPC, adicione uma rota com o destino de `0.0.0.0/0` para tráfego IPv4 ou `::/0` para tráfego IPv6 e um alvo do ID do gateway da Internet (`igw-xxxxxxxxxxxxxxxxx`).

Destino	Destino
0.0.0.0/0	*igw-id*
::/0	*igw-id*

Para obter mais informações, consulte Habilitar o acesso da VPC à Internet usando gateways da Internet.

Roteamento para um dispositivo NAT

Para permitir que instâncias em uma sub-rede privada se conectem à Internet, você pode criar um gateway NAT ou executar uma instância NAT em uma sub-rede pública. Depois, adicione uma rota para a tabela de rotas da sub-rede privada que roteia o tráfego de Internet IPv4 (`0.0.0.0/0`) para o dispositivo NAT.

Destino	Destino
0.0.0.0/0	*nat-gateway-id*

Você também pode criar rotas mais específicas para outros alvos para evitar cobranças desnecessárias de processamento de dados pelo uso de um gateway NAT ou para rotear determinado tráfego de forma privada. No exemplo a seguir, o tráfego do Amazon S3 (pl-xxxxxxxxxx, uma lista de prefixos que contém os intervalos de endereços IP do Amazon S3 em uma região específica) é roteado para um endpoint de VPC de gateway e o tráfego 10.25.0.0/16 é roteado para uma conexão de emparelhamento de VPC. Esses intervalos de endereços IP são mais específicos do que 0.0.0.0/0. Quando as instâncias enviam tráfego para o Amazon S3 ou para a VPC de emparelhamento, o tráfego é enviado para o VPC endpoint do gateway ou para a conexão de emparelhamento da VPC. O restante do tráfego é enviado para o gateway NAT.

Destino	Destino
0.0.0.0/0	*nat-gateway-id*
pl-*xxxxxxxx*	*vpce-id*
10.25.0.0/16	*pcx-id*

Para ter mais informações, consulte Dispositivos NAT.

Roteamento para um gateway privado virtual

Você pode usar uma conexão do AWS Site-to-Site VPN para permitir que as instâncias em sua VPC se comuniquem com sua rede. Para fazer isso, crie e anexe um gateway privado virtual à VPC.

Depois, adicione uma rota na tabela de rotas de sub-rede com o destino da rede e um alvo para o gateway privado virtual (`vgw-xxxxxxxxxxxxxxxxx`).

Destino	Destino
10.0.0.0/16	*vgw-id*

É possível então criar e configurar sua conexão do Site-to-Site VPN. Para obter mais informações, consulte O que é AWS Site-to-Site VPN? e Tabelas de rotas e prioridade de rotas da VPN no Manual do usuário do AWS Site-to-Site VPN.

Uma conexão do Site-to-Site VPN em um gateway privado virtual não é compatível com o tráfego IPv6. Entretanto, oferecemos compatibilidade para tráfego IPv6 roteado por meio de um gateway privado virtual para uma conexão do AWS Direct Connect. Para obter mais informações, consulte o Manual do usuário do AWS Direct Connect.

Roteamento para um gateway local do AWS Outposts

Esta seção descreve as configurações da tabela de rotas para roteamento para um gateway local do AWS Outposts.

Conteúdo

- Habilitar o tráfego entre as sub-redes do Outpost e sua rede on-premises
- Habilitar o tráfego entre sub-redes na mesma VPC entre Outposts

Habilitar o tráfego entre as sub-redes do Outpost e sua rede on-premises

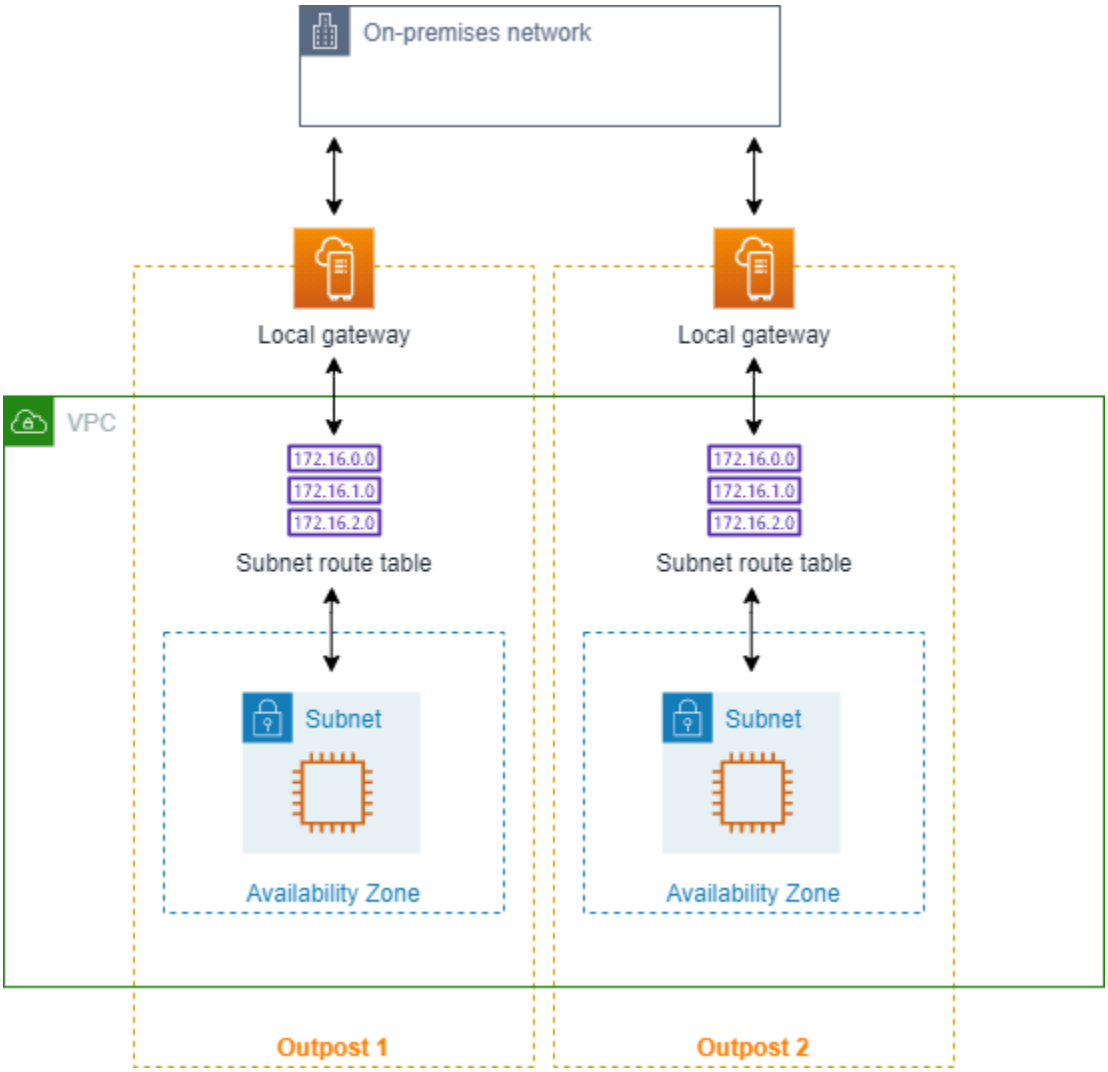
As sub-redes que estão em VPCs associadas ao AWS Outposts podem ter um tipo de destino adicional de um gateway local. Considere o caso em que você deseja ter o tráfego de roteamento de gateway local com um endereço de destino de 192.168.10.0/24 para a rede do cliente. Para fazer isso, adicione a seguinte rota com a rede de destino e um alvo do gateway local (`lgw-xxxx`).

Destino	Destino
192.168.10.0/24	*lgw-id*

Habilitar o tráfego entre sub-redes na mesma VPC entre Outposts

Você pode estabelecer comunicação entre sub-redes que estão na mesma VPC entre diferentes Outposts usando os gateways locais do Outpost e sua rede on-premises.

Você pode usar esse atributo para criar arquiteturas semelhantes às arquiteturas de várias zonas de disponibilidade (AZ) para suas aplicações on-premises executadas em racks do Outposts ao estabelecer conectividade entre racks do Outposts que estão ancorados em diferentes AZs.



Para habilitar esse atributo, adicione uma rota à tabela de rotas de sub-rede do rack do Outpost que seja mais específica do que a rota local dessa tabela de rotas e tenha um tipo de gateway local de destino. O destino da rota deve corresponder a todo o bloco IPv4 da sub-rede na sua VPC que esteja em outro Outpost. Repita essa configuração para todas as sub-redes do Outpost que precisam se comunicar.

Important

- Para usar esse atributo, você deve usar o roteamento direto de VPC. Você não pode usar seus próprios endereços IP de propriedade do cliente.
- Sua rede on-premises à qual os gateways locais do Outposts estão conectados deve ter o roteamento necessário para que as sub-redes possam acessar umas às outras.
- Se quiser usar grupos de segurança para recursos nas sub-redes, você deverá usar regras que incluam intervalos de endereços IP como origem ou destino nas sub-redes do Outpost. Você não pode usar IDs de grupos de segurança.
- Os racks existentes do Outposts podem precisar de uma atualização para permitir o suporte à comunicação intra-VPC entre vários Outposts. Se esse atributo não funcionar para você, entre em contato com o suporte da AWS.

Example Exemplo

Para uma VPC com CIDR de 10.0.0.0/16, uma sub-rede do Outpost 1 com CIDR de 10.0.1.0/24 e uma sub-rede do Outpost 2 com CIDR de 10.0.2.0/24, a entrada para a tabela de rotas da sub-rede do Outpost 1 será a seguinte:

Destino	Destino
10.0.0.0/16	Local
10.0.2.0/24	*lgw-1-id*

A entrada para a tabela de rotas da sub-rede do Outpost 2 será a seguinte:

Destino	Destino
10.0.0.0/16	Local
10.0.1.0/24	*lgw-2-id*

Roteamento para uma conexão de emparelhamento de VPC

Conexão de emparelhamento da VPC é uma conexão de redes entre duas VPCs que permite direcionar o tráfego entre elas usando endereços IPv4 privados. As instâncias em qualquer VPC podem se comunicar umas com as outras como se estivessem na mesma rede.

Para habilitar o roteamento de tráfego entre VPCs em uma conexão de emparelhamento de VPC, você deve adicionar uma rota a uma ou mais tabelas de rotas de sub-rede que direcione para a conexão de emparelhamento da VPC. Isso permite que você acesse todo ou parte do bloco CIDR da outra VPC na conexão de emparelhamento. Do mesmo modo, o proprietário da outra VPC deve adicionar uma rota à tabela de rotas de sub-rede dele para rotear o tráfego de volta para a sua VPC.

Por exemplo, você tem uma conexão de emparelhamento da VPC (`pcx-11223344556677889`) entre duas VPCs, com as seguintes informações:

- VPC A: o bloco CIDR é 10.0.0.0/16
- VPC B: o bloco CIDR é 172.31.0.0/16

Para permitir o tráfego entre as VPCs e acesso a todo o bloco CIDR IPv4 de qualquer uma das VPCs, a tabela de rotas da VPC A é configurada da forma a seguir.

Destino	Destino
10.0.0.0/16	Local
172.31.0.0/16	pcx-11223344556677889

A tabela de rotas da VPC B é configurada da forma a seguir.

Destino	Destino
172.31.0.0/16	Local
10.0.0.0/16	pcx-11223344556677889

Sua conexão de emparelhamento da VPC também pode oferecer suporte à comunicação IPv6 entre instâncias nas VPCs, desde que as VPCs e as instâncias estejam habilitadas para comunicação

IPv6. Para permitir o roteamento de tráfego IPv6 entre VPCs, você deve adicionar uma rota para sua tabela de rotas direcionada para a conexão de emparelhamento da VPC para acessar todo ou parte do bloco CIDR IPv6 da VPC emparelhada.

Por exemplo, usando a mesma conexão de emparelhamento da VPC (`pcx-11223344556677889`) anterior, presuma que as VPCs tenham as seguintes informações:

- VPC A: o bloco CIDR IPv6 é `2001:db8:1234:1a00::/56`
- VPC B: o bloco CIDR IPv6 é `2001:db8:5678:2b00::/56`

Para permitir a comunicação IPv6 na conexão de emparelhamento de VPC, adicione a rota a seguir à tabela de rotas de sub-rede da VPC A.

Destino	Destino
10.0.0.0/16	Local
172.31.0.0/16	pcx-11223344556677889
2001:db8:5678:2b00::/56	pcx-11223344556677889

Adicione a rota a seguir à tabela de rotas da VPC B.

Destino	Destino
172.31.0.0/16	Local
10.0.0.0/16	pcx-11223344556677889
2001:db8:1234:1a00::/56	pcx-11223344556677889

Para obter mais informações sobre conexões de emparelhamento de VPC, consulte o Guia de emparelhamento da Amazon VPC.

Roteamento para um VPC endpoint de gateway

Um VPC endpoint de gateway permite criar uma conexão privada entre sua VPC e outro serviço da AWS. Ao criar um endpoint de gateway, você especifica as tabelas de rota de sub-rede em sua VPC

que são usadas pelo endpoint do gateway. Uma rota é automaticamente adicionada a cada uma das tabelas de rotas com um destino que especifica o ID da lista de prefixos do serviço (`pl-xxxxxxxx`) e um destino com o ID do endpoint (`vpce-xxxxxxxxxxxxxxxxx`). Você não pode excluir nem modificar explicitamente a rota do endpoint, mas pode alterar as tabelas de rotas que são usadas pelo endpoint.

Para obter mais informações sobre roteamento para endpoints e as implicações com relação a rotas para os serviços da AWS, consulte Roteamento para endpoints de gateway.

Roteamento para um gateway da Internet apenas de saída

Você pode criar um gateway da Internet apenas de saída para sua VPC a fim de permitir que instâncias em uma sub-rede privada iniciem comunicação de saída com a Internet, mas impedir que a Internet inicie conexões com essas instâncias. Só se usa o gateway da Internet apenas de saída para tráfego IPv6. Para configurar o roteamento para um gateway de Internet apenas de saída, adicione uma rota à tabela de rotas da sub-rede privada que roteie o tráfego de Internet IPv6 (`::/0`) para o gateway da Internet apenas de saída.

Destino	Destino
::/0	*eigw-id*

Para obter mais informações, consulte Habilitar o tráfego IPv6 de saída usando gateways da Internet somente de saída.

Roteamento para um gateway de trânsito

Ao anexar uma VPC a um gateway de trânsito, você deverá adicionar uma rota à sua tabela de rotas de sub-rede para que o tráfego seja roteado pelo gateway de trânsito.

Pense no seguinte cenário, no qual você tem três VPCs anexadas a um gateway de trânsito. Nesse caso, todos os anexos estão associados à tabela de rotas do gateway de trânsito e a propagam. Sendo assim, todos os anexos podem rotear pacotes uns para os outros, e o gateway de trânsito funciona como um simples hub com IPs da camada 3.

Por exemplo, você tem duas VPCs com a seguinte informação:

- VPC A: 10.1.0.0/16, anexo ID tgw-attach-11111111111111111
- VPC B: 10.2.0.0/16, anexo ID tgw-attach-22222222222222222

Para permitir o tráfego entre as VPCs e o acesso ao gateway de trânsito, a tabela de rotas A da VPC A é configurada da forma a seguir.

Destino	Destino
10.1.0.0/16	local
10.0.0.0/8	*tgw-id*

Veja a seguir entradas demonstrativas de uma tabela de rotas do gateway de trânsito para os anexos da VPC.

Destino	Destino
10.1.0.0/16	tgw-attach-11111111111111111
10.2.0.0/16	tgw-attach-22222222222222222

Para obter mais informações sobre tabelas de rotas de gateway de trânsito, consulte Rotear em Gateways de trânsito da Amazon VPC.

Roteamento para um dispositivo Middlebox

Você pode adicionar dispositivos middlebox aos caminhos de roteamento para sua VPC. Alguns possíveis casos de uso são:

- Interceptar o tráfego que entra na VPC por meio de um gateway da Internet ou de um gateway privado virtual direcionando-o para um dispositivo middlebox na VPC. Você pode usar o assistente de roteamento do middlebox para que a AWS configure automaticamente as tabelas de rota apropriadas para seu gateway, middlebox e sub-rede de destino. Para ter mais informações, consulte the section called “Assistente de roteamento do middlebox”.
- Direcionar tráfego entre duas sub-redes para um dispositivo middlebox. Você pode fazer isso criando uma rota para a tabela de rotas de uma sub-rede que corresponda ao CIDR de sub-rede da outra sub-rede e especifique um endpoint do balanceador de carga do gateway, um gateway NAT, um endpoint de Network Firewall ou a interface de rede de um dispositivo como destino. Como alternativa, para redirecionar todo o tráfego da sub-rede para qualquer outra sub-rede,

substitua o destino da rota local por um endpoint do balanceador de carga do gateway, gateway NAT ou interface de rede.

Você pode configurar o dispositivo para atender às suas necessidades. Por exemplo, você pode configurar um dispositivo de segurança que monitora todo o tráfego ou um dispositivo de aceleração WAN. O dispositivo é implantado como uma instância do Amazon EC2 em uma sub-rede na VPC e é representado por uma interface de rede elástica (interface de rede) na sub-rede.

Se você habilitar a propagação de rotas para a tabela de rotas da sub-rede de destino, esteja ciente da prioridade das rotas. Priorizamos a rota mais específica e se as rotas corresponderem, priorizamos as rotas estáticas sobre as rotas propagadas. Revise as suas rotas para garantir que o tráfego seja encaminhado corretamente e que não há consequências não intencionais caso você habilite ou desabilite a propagação de rotas (por exemplo, a propagação de rotas é obrigatória para uma conexão do AWS Direct Connect que oferece suporte a quadros jumbo).

Para rotear o tráfego de entrada da VPC para um dispositivo, associe uma tabela de rotas ao gateway da Internet ou ao gateway privado virtual e especifique a interface de rede do seu dispositivo como alvo para o tráfego da VPC. Para ter mais informações, consulte Tabelas de rotas do gateway. Você também pode rotear o tráfego de saída da sub-rede para um dispositivo middlebox em outra sub-rede.

Para exemplos de roteamento de middlebox, consulte Cenários de middlebox.

Conteúdo

Considerações sobre o dispositivo

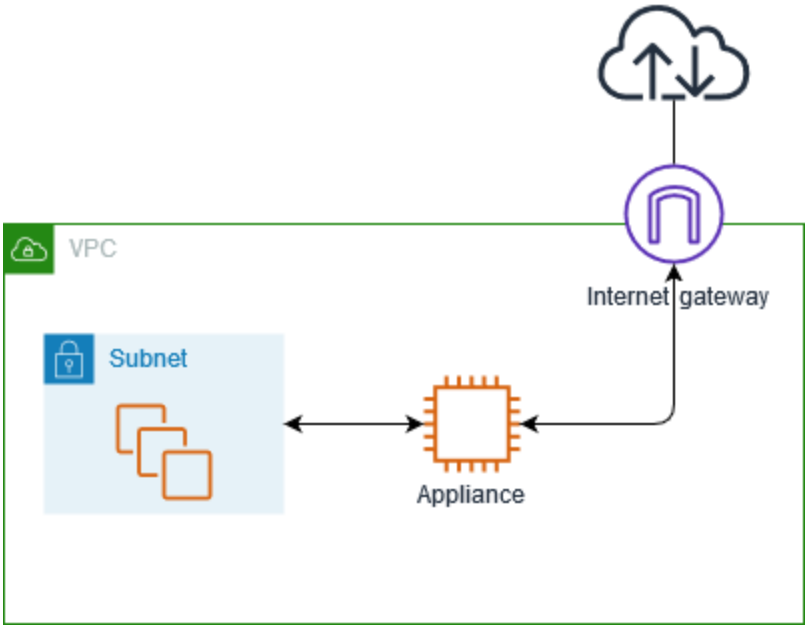
Você pode escolher um dispositivo de terceiros em AWS Marketplace ou configurar seu próprio dispositivo. Ao criar ou configurar um dispositivo, observe o seguinte:

- O dispositivo deve ser configurado em uma sub-rede separada para o tráfego de origem ou de destino.
- Você deve desabilitar a verificação de origem/destino no dispositivo. Para obter mais informações, consulte Alterar a verificação da origem ou destino no Guia do usuário do Amazon EC2.

- Você não pode rotear o tráfego entre hosts na mesma sub-rede por meio de um dispositivo.
- O dispositivo não precisa executar a conversão de endereços de rede (NAT).
- Você pode adicionar uma rota às suas tabelas de rotas que seja mais específica do que a rota local. Você pode usar rotas mais específicas para redirecionar tráfego entre sub-redes em uma VPC (tráfego leste-oeste) para um dispositivo middlebox. O destino da rota deve corresponder a todo o bloco CIDR IPv4 ou IPv6 de uma sub-rede em sua VPC.
- Para interceptar tráfego IPv6, certifique-se de que sua VPC, sub-rede e o dispositivo oferecem suporte a IPv6.

Roteamento de tráfego entre um gateway e um dispositivo

Para rotear o tráfego de entrada da VPC para um dispositivo, associe uma tabela de rotas ao gateway da Internet ou ao gateway privado virtual e especifique a interface de rede do seu dispositivo como alvo para o tráfego da VPC. No exemplo a seguir, a VPC tem um gateway da Internet, um dispositivo e uma sub-rede com instâncias. O tráfego da Internet é roteado por meio de um dispositivo.



Associe esta tabela de rotas ao seu gateway da Internet ou gateway privado virtual. A primeira entrada é a rota local. A segunda entrada envia tráfego IPv4 destinado à sub-rede para a interface de rede do dispositivo. Essa rota é mais específica do que a rota local padrão.

Destino	Alvo
CIDR DA VPC	Local
CIDR da sub-rede	*ID da interface de rede do dispositivo*

Como alternativa, você pode substituir o destino da rota local pela interface de rede do dispositivo. Você pode fazer isso para garantir que todo o tráfego seja roteado automaticamente para o dispositivo, incluindo o tráfego destinado a sub-redes que serão adicionadas à VPC no futuro.

Destino	Alvo
CIDR DA VPC	*ID da interface de rede do dispositivo*

Para rotear o tráfego da sub-rede para um dispositivo em outra sub-rede, adicione uma rota à tabela de rotas de sub-rede que roteia o tráfego para a interface de rede do dispositivo. O destino deve ser menos específico do que o destino da rota local. Por exemplo, para o tráfego destinado à Internet, especifique `0.0.0.0/0` (todos os endereços IPv4) para o destino.

Destino	Alvo
CIDR DA VPC	Local
0.0.0.0/0	*ID da interface de rede do dispositivo*

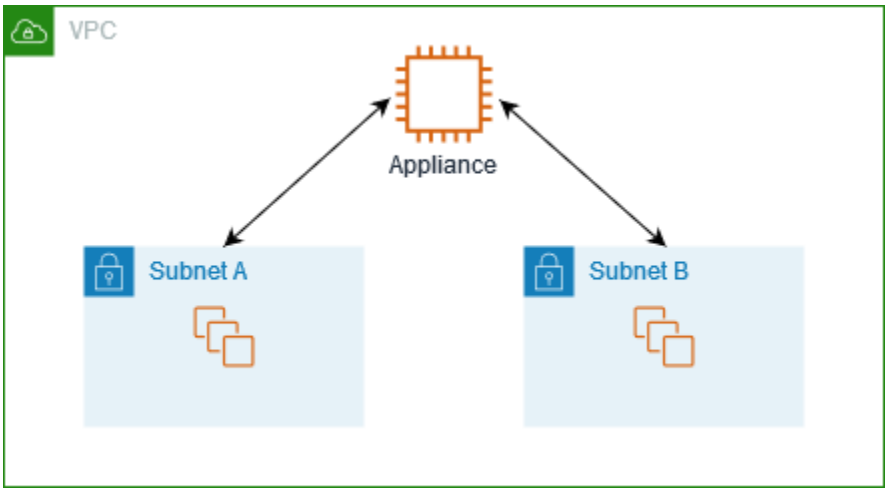
Na tabela de rotas associada à sub-rede do dispositivo, adicione uma rota que envie o tráfego de volta para o gateway da Internet ou para o gateway privado virtual.

Destino	Alvo
CIDR DA VPC	Local

Destino	Alvo
0.0.0.0/0	*igw-id*

Roteamento do tráfego entre sub-redes para um dispositivo

Você pode rotear o tráfego destinado a uma sub-rede específica para a interface de rede de um dispositivo. No exemplo a seguir, a VPC contém duas sub-redes e um dispositivo. O tráfego entre as sub-redes é roteado por meio de um dispositivo.



Grupos de segurança

Quando você roteia o tráfego entre instâncias em sub-redes diferentes por meio de um dispositivo middlebox, os grupos de segurança de ambas as instâncias devem permitir que o tráfego flua entre as instâncias. O grupo de segurança para cada instância deve fazer referência ao endereço IP privado da outra instância ou ao intervalo CIDR da sub-rede que contém a outra instância, como a origem. Se você fizer referência ao grupo de segurança da outra instância como a origem, isso não permitirá que o tráfego flua entre as instâncias.

Roteamento

A seguir é apresentado um exemplo de tabela de rotas para a sub-rede A. A primeira entrada permite que as instâncias na VPC comuniquem-se entre si. A segunda entrada roteia todo o tráfego da sub-rede A para a sub-rede B para a interface de rede do dispositivo.

Destino	Alvo
CIDR DA VPC	Local
CIDR da sub-rede B	*ID da interface de rede do dispositivo*

A seguir é apresentado um exemplo de tabela de rotas para a sub-rede B. A primeira entrada permite que as instâncias na VPC comuniquem-se entre si. A segunda entrada roteia todo o tráfego da sub-rede B para a sub-rede A para a interface de rede do dispositivo.

Destino	Alvo
CIDR DA VPC	Local
CIDR da sub-rede A	*ID da interface de rede do dispositivo*

Como alternativa, você pode substituir o destino da rota local pela interface de rede do dispositivo. Você pode fazer isso para garantir que todo o tráfego seja roteado automaticamente para o dispositivo, incluindo o tráfego destinado a sub-redes que serão adicionadas à VPC no futuro.

Destino	Alvo
CIDR DA VPC	*ID da interface de rede do dispositivo*

Roteamento com uma lista de prefixos

Se você faz com frequência referência ao mesmo conjunto de blocos CIDR nos recursos da AWS, poderá criar uma lista de prefixos gerenciados pelo cliente para agrupá-los. Depois, você pode especificar a lista de prefixos como destino na entrada da tabela de rotas. Posteriormente, você pode adicionar ou remover entradas na lista de prefixos sem precisar atualizar as tabelas de rotas.

Por exemplo, você tem um gateway de trânsito com vários anexos de VPC. As VPCs devem ser capazes de se comunicar com dois anexos de VPC específicos que tenham os blocos CIDR a seguir:

- 10.0.0.0/16
- 10.2.0.0/16

Crie uma lista de prefixos com as duas entradas. Nas tabelas de rota de sub-rede, crie uma rota e especifique a lista de prefixos como destino e o gateway de trânsito como destino.

Destino	Destino
172.31.0.0/16	Local
pl-123abc123abc123ab	*tgw-id*

O número máximo de entradas para as listas de prefixos é equivalente ao número de entradas na tabela de rotas.

Roteamento para um endpoint do Gateway Load Balancer

Um Gateway Load Balancer permite distribuir tráfego para uma frota de dispositivos virtuais, como firewalls. É possível criar um Gateway Load Balancer, configurar um serviço de endpoint para o Gateway Load Balancer e, em seguida, criar um endpoint para o Gateway Load Balancer em sua VPC com a finalidade de estabelecer a conexão com o serviço.

Para rotear seu tráfego para o Gateway Load Balancer (por exemplo, para inspeção de segurança), especifique o endpoint do Gateway Load Balancer como destino nas tabelas de rotas.

Para obter um exemplo de dispositivos de segurança por trás de um balanceador de carga de gateway, consulte the section called “Inspecionar o tráfego usando dispositivos de segurança”.

Para especificar o endpoint do Gateway Load Balancer na tabela de rotas, use o ID do VPC endpoint. Por exemplo, para rotear tráfego para 10.0.1.0/24 para um endpoint de balanceador de carga de gateway, adicione a rota a seguir.

Destino	Alvo
10.0.1.0/24	*vpc-endpoint-id*

Para obter mais informações, consulte Balanceadores de carga de gateway.

Alterar a tabela de rotas de uma sub-rede

Esta seção explica como trabalhar com tabelas de rotas. Observe que esta seção é um agrupamento de procedimentos, todos relacionados à realização de alterações na tabela de rotas de sub-rede.

Conteúdo

Determinar a tabela de rotas para uma sub-rede

É possível determinar a qual tabela de rotas uma sub-rede está associada examinando os detalhes sobre a sub-rede no console da Amazon VPC.

Para determinar a tabela de rotas para uma sub-rede

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Sub-redes.
3. Selecione a sub-rede.
4. Escolha a guia Route Table (Tabela de rotas) para visualizar as informações da tabela e as respectivas rotas. Para determinar se a associação com a tabela de rotas principal existe e é explícita, consulte Determinar as sub-redes e/ou os gateways explicitamente associadas.

Determinar as sub-redes e/ou os gateways explicitamente associadas

Você pode determinar quantas e quais sub-redes ou gateways estão associados explicitamente a uma tabela de rotas.

A tabela de rotas principal pode ter associações explícitas e implícitas de sub-rede. A tabela de rotas personalizada pode ter somente associações explícitas.

As sub-redes que não estão associadas explicitamente a nenhuma tabela de rotas têm uma associação implícita com a tabela de rotas principal. Você pode associar explicitamente uma sub-rede à tabela de rotas principal. Para obter um exemplo de por que você pode fazer isso, consulte Substituir a tabela de rotas principal.

Para determinar quais sub-redes estão explicitamente associadas usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Route tables.
3. Verifique a coluna Explicit subnet association (Associação de sub-rede explícita) para determinar as sub-redes explicitamente associadas e a coluna Main (Principal) para determinar se essa é a tabela de rotas principal.
4. Selecione a tabela de rotas e escolha a guia Subnet associations (Associações de sub-rede).
5. As sub-redes em Explicit subnet associations (Associações de sub-rede explícitas) são explicitamente associados à tabela de rotas. As sub-redes em Subnets without explicit associations (Sub-redes sem associações explícitas) pertencem à mesma VPC que a tabela de rotas, mas não estão associadas a nenhuma tabela de rotas, portanto, são associadas implicitamente à tabela de rotas principal para a VPC.

Para determinar quais gateways estão explicitamente associados usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Route tables.
3. Selecione a tabela de rotas e escolha a guia Edge associations (Associações de borda).

Para descrever uma ou mais tabelas de rotas e exibir suas associações usando a linha de comando

- describe-route-tables (AWS CLI)
- Get-EC2RouteTable (AWS Tools for Windows PowerShell)

Criar uma tabela de rotas personalizada

É possível criar uma tabela de rotas personalizada para sua VPC usando o console da Amazon VPC.

> **Note**
>
> Existe uma cota em relação ao número de tabelas de rotas que podem ser criadas por VPC. Também existe uma cota em relação ao número de rotas que pode ser adicionadas por tabela de rotas. Para ter mais informações, consulte Cotas da Amazon VPC.

Para criar uma tabela de rotas personalizada usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Route tables.
3. Escolha Create Route Table (Criar tabela de rotas).
4. (Opcional) Em Name (Nome), insira um nome para a tabela de rotas.
5. Em VPC, escolha sua VPC.
6. (Opcional) Para adicionar uma etiqueta, escolha Add new tag (Adicionar nova etiqueta) e insira a chave e o valor da etiqueta.
7. Escolha Create Route Table (Criar tabela de rotas).

Para criar uma tabela de rotas personalizada usando a linha de comando

- create-route-table (AWS CLI)
- New-EC2RouteTable (AWS Tools for Windows PowerShell)

Adicionar e remover rotas de uma tabela de rotas

Você pode adicionar, excluir e modificar rotas em suas tabelas de rotas. Você só pode modificar rotas que você tenha adicionado.

Para obter mais informações sobre como trabalhar com rotas estáticas para uma conexão da Site-to-Site VPN, consulte Edição de rotas estáticas para uma conexão da Site-to-Site VPN no Manual do usuário da AWS Site-to-Site VPN.

> **Note**
>
> Existe uma cota em relação ao número de tabelas de rotas que podem ser criadas por VPC. Também existe uma cota em relação ao número de rotas que pode ser adicionadas por tabela de rotas. Para ter mais informações, consulte Cotas da Amazon VPC.

Para atualizar as rotas de uma tabela de rotas usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Route Tables (Tabelas de rotas) e selecione a tabela de rotas.
3. Selecione Actions (Ações), Edit routes (Editar rotas).
4. Para adicionar uma rota, escolha Add route (Adicionar rota). Em Destino insira o bloco CIDR de destino, um único endereço IP ou o ID de uma lista de prefixos.
5. Para modificar uma rota, em Destination (Destino), substitua o bloco CIDR de destino ou o endereço IP único. Em Target (alvo), escolha um alvo.
6. Para excluir uma rota, escolha Remove (Remover).
7. Escolha Salvar alterações.

Para atualizar as rotas de uma tabela de rotas usando a linha de comando

- create-route (AWS CLI)
- replace-route (AWS CLI)
- delete-route (AWS CLI)
- New-EC2Route (AWS Tools for Windows PowerShell)
- Set-EC2Route (AWS Tools for Windows PowerShell)
- Remove-EC2Route (AWS Tools for Windows PowerShell)

> **Note**
>
> Se você adicionar uma rota usando uma ferramenta de linha de comando ou a API, o bloco CIDR de destino será automaticamente modificado para sua forma canônica. Por exemplo, se você especificar `100.68.0.18/18` para o bloco CIDR, criaremos uma rota com um bloco CIDR de destino de `100.68.0.0/18`.

Habilite ou desabilite a propagação de rotas.

A propagação de rotas permite que um gateway privado virtual propague automaticamente rotas para suas tabelas de rotas. Isso significa que você não precisará adicionar ou remover rotas VPN manualmente.

Para concluir esse processo, você deve ter um gateway privado virtual.

Para mais informações, consulte Opções de roteamento do Site-to-Site VPN no Guia do usuário do Site-to-Site VPN.

Para ativar a propagação de rotas usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Route Tables (Tabelas de rotas) e selecione a tabela de rotas.
3. Selecione Actions (Ações), Edit route propagation (Editar propagação de rota).
4. Marque a caixa de seleção Enable (Habilitar) próxima ao gateway privado virtual e escolha Save (Salvar).

Para ativar a propagação de rotas usando a linha de comando

- enable-vgw-route-propagation (AWS CLI)
- Enable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

Para desativar a propagação de rotas usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Route Tables (Tabelas de rotas) e selecione a tabela de rotas.
3. Selecione Actions (Ações), Edit route propagation (Editar propagação de rota).
4. Desmarque a caixa de seleção Enable (Habilitar) próxima ao gateway privado virtual e escolha Save (Salvar).

Para desativar a propagação de rotas usando a linha de comando

- disable-vgw-route-propagation (AWS CLI)
- Disable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

Alterar a tabela de rotas para uma sub-rede

Você pode alterar a associação da tabela de rotas para uma sub-rede.

Quando você altera a tabela de rotas, as conexões existentes na sub-rede são descartadas, a menos que a nova tabela de rotas contenha uma rota do mesmo tráfego para o mesmo destino.

Para alterar uma associação de tabela de rotas de sub-rede usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Subnets e selecione a sub-rede.
3. Na guia Route Table (Tabela de rotas) escolha Edit route table association (Editar associação de tabela de rotas).
4. Para Route table ID (ID da tabela de rotas), selecione a nova tabela de rotas.
5. Escolha Salvar.

Para alterar a tabela de rotas associada a uma sub-rede usando a linha de comando

- replace-route-table-association (AWS CLI)
- Set-EC2RouteTableAssociation (AWS Tools for Windows PowerShell)

Associar ou desassociar uma sub-rede de uma tabela de rotas

Para destinar rotas de uma tabela a uma sub-rede específica, você deve associar a tabela de rotas à sub-rede. Uma tabela de rotas pode ser associada a várias sub-redes. No entanto, uma sub-rede só pode ser associada a uma tabela de rotas por vez. Por padrão, qualquer sub-rede não associada explicitamente a uma tabela está associada implicitamente à tabela de rotas principal.

Você pode dissociar uma sub-rede de uma tabela de rotas. Enquanto você não associa a sub-rede com outra tabela de rotas, ela se mantém associada implicitamente à tabela de rotas principal.

Para associar ou desassociar uma tabela de rotas de uma sub-rede usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Route Tables (Tabelas de rotas) e selecione a tabela de rotas.
3. Na guia Subnet Associations (Associações da sub-rede) selecione Edit subnet associations (Editar associações da sub-rede).

4. Marque ou desmarque a caixa de seleção para a sub-rede que será associada à ou desassociada da tabela de rotas.
5. Selecione Salvar associações.

Para associar uma sub-rede a uma tabela de rotas usando a linha de comando

- associate-route-table (AWS CLI)
- Register-EC2RouteTable (AWS Tools for Windows PowerShell)

Para desassociar uma sub-rede de uma tabela de rotas usando a linha de comando

- disassociate-route-table (AWS CLI)
- Unregister-EC2RouteTable (AWS Tools for Windows PowerShell)

Substituir a tabela de rotas principal

Esta seção descreve como alterar qual tabela de rotas é a tabela de rotas principal em sua VPC.

Para substituir a tabela de rotas principal usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Route Tables (Tabelas de rotas) e selecione a nova tabela de rotas principal.
3. Escolha Actions (Ações), Set main route table (Definir tabela de rotas principal).
4. Quando a confirmação for solicitada, insira **`set`** e escolha OK.

Para substituir a tabela de rotas principal usando a linha de comando

- replace-route-table-association (AWS CLI)
- Set-EC2RouteTableAssociation (AWS Tools for Windows PowerShell)

O procedimento a seguir descreve como remover uma associação explícita entre uma sub-rede e a tabela de rotas principal. O resultado é uma associação implícita entre a sub-rede e a tabela de rotas principal. O processo é o mesmo realizado para dissociar qualquer sub-rede de uma tabela de rotas.

Para remover uma associação explícita a uma tabela de rotas principal

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Route Tables (Tabelas de rotas) e selecione a tabela de rotas.
3. Na guia Subnet Associations (Associações da sub-rede) selecione Edit subnet associations (Editar associações da sub-rede).
4. Desmarque a caixa de seleção da sub-rede.
5. Selecione Salvar associações.

Controle o tráfego que entra na sua VPC com uma tabela de rotas de gateway

Para controlar o tráfego que entra em sua VPC com uma tabela de rotas de gateway, é possível associar ou desassociar um gateway da Internet ou um gateway privado virtual de uma tabela de rotas. Para ter mais informações, consulte Tabelas de rotas do gateway.

Para associar ou desassociar um gateway de uma tabela de rotas usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Route Tables (Tabelas de rotas) e selecione a tabela de rotas.
3. Na guia Edge Associations (Associações da borda) selecione Edit edge associations (Editar associações da borda).
4. Marque ou desmarque a caixa de seleção do gateway.
5. Escolha Salvar alterações.

Para associar ou desassociar um gateway de uma tabela de rotas usando a AWS CLI

Use o comando associate-route-table. O exemplo a seguir associa o gateway da Internet `igw-11aa22bb33cc44dd1` à tabela de rotas `rtb-01234567890123456`.

```
aws ec2 associate-route-table --route-table-id rtb-01234567890123456 --gateway-id
 igw-11aa22bb33cc44dd1
```

Para desassociar um gateway de uma tabela de rotas usando a linha de comando

- disassociate-route-table (AWS CLI)

- Unregister-EC2RouteTable (AWS Tools for Windows PowerShell)

Substituir ou restaurar o destino de uma rota local

Você pode alterar o destino da rota local padrão. Se você substituir o alvo de uma rota local, poderá restaurá-lo posteriormente para o alvo `local` padrão. Se sua VPC tiver vários blocos CIDR, suas tabelas de rotas terão várias rotas locais: uma por bloco CIDR. Você pode substituir ou restaurar o alvo de cada uma das rotas locais conforme necessário.

Para atualizar a rota local usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Route Tables (Tabelas de rotas) e selecione a tabela de rotas.
3. Na guia Routes (Rotas), escolha Edit routes (Editar rotas).
4. Para a rota local, desmarque Target (Destino) e escolha um novo destino.
5. Escolha Salvar alterações.

Para restaurar o alvo de uma rota local usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Route Tables (Tabelas de rotas) e selecione a tabela de rotas.
3. Selecione Actions (Ações), Edit routes (Editar rotas).
4. Para a rota local, desmarque Target (Destino) e, em seguida, escolha local.
5. Escolha Salvar alterações.

Para substituir o alvo por uma rota local usando a AWS CLI

Use o comando replace-route. O exemplo a seguir substitui o alvo da rota local por `eni-11223344556677889`.

```
aws ec2 replace-route --route-table-id rtb-01234567890123456 --destination-cidr-block
 10.0.0.0/16 --network-interface-id eni-11223344556677889
```

Para restaurar o alvo de uma rota local usando a AWS CLI

O exemplo a seguir restaura o alvo local para a tabela de rotas `rtb-01234567890123456`.

```
aws ec2 replace-route --route-table-id rtb-01234567890123456 --destination-cidr-block
 10.0.0.0/16 --local-target
```

Solucionar problemas de acessibilidade

O Reachability Analyzer é uma ferramenta de análise de configuração estática. Use o Reachability Analyzer para analisar e depurar a acessibilidade da rede entre dois recursos em sua VPC. O Reachability Analyzer produz detalhes salto a salto do caminho virtual entre esses recursos quando eles estão acessíveis e identifica o componente responsável pelo bloqueio quando eles estão inacessíveis. Por exemplo, ele pode identificar rotas de tabela de rotas ausentes ou mal configuradas.

Para obter mais informações, consulte o Guia do Analisador de Acessabilidade.

Assistente de roteamento do middlebox

Se você deseja configurar o controle refinado sobre o caminho de roteamento do tráfego entrando ou saindo da VPC, por exemplo, redirecionando o tráfego para um dispositivo de segurança, você pode usar o assistente de roteamento de middlebox no console da VPC. O assistente de roteamento do middlebox ajuda você criando automaticamente as tabelas de rotas e as rotas (saltos) necessárias para redirecionar o tráfego conforme necessário.

O assistente de roteamento do middlebox pode ajudar a configurar o roteamento para os seguintes cenários:

- Roteamento de tráfego para um dispositivo middlebox, por exemplo, uma instância do Amazon EC2 configurada como um dispositivo de segurança.
- Roteamento de tráfego para um balanceador de carga de gateway. Para obter mais informações, consulte o Guia do usuário para balanceadores de carga de gateway .

Para ter mais informações, consulte the section called “Cenários de middlebox”.

Conteúdo

Pré-requisitos do assistente de roteamento do Middlebox

Consulte the section called “Considerações do assistente de roteamento do middleboxo”. Em seguida, certifique-se de ter as seguintes informações disponíveis antes de usar o assistente de roteamento do middlebox.

- A VPC.
- O recurso do qual o tráfego é proveniente ou por meio do qual entra na VPC, por exemplo, um gateway da Internet, um gateway privado virtual ou uma interface de rede.
- A interface de rede do middlebox ou o endpoint do balanceador de carga do gateway.
- A sub-rede de destino para o tráfego.

Redirecione o tráfego da VPC para um dispositivo de segurança

O assistente de roteamento do middlebox está disponível no Amazon Virtual Private Cloud Console.

Conteúdo

1. Criar rotas usando o assistente de roteamento do middlebox

Para criar rotas usando o assistente de roteamento do middlebox

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Selecione sua VPC e escolha Actions (Ações), Manage middlebox routes (Gerenciar rotas do middlebox).
4. Escolha Create routes (Criar rotas).
5. Na página Specify routes (Especificar rotas), faça o seguinte:

    - Em Source (Origem), escolha a origem do seu tráfego. Se você escolher um gateway privado virtual, para Destination IPv4 CIDR (CIDR IPv4 de destino), insira o CIDR para o tráfego on-premises que entra na VPC pelo gateway privado virtual.

- Em Middlebox, escolha o ID da interface de rede associado ao dispositivo middlebox ou, ao usar um endpoint de balanceador de carga do gateway, escolha o ID do endpoint da VPC.
- Em Destination subnet (Sub-rede de destino), escolha a sub-rede de destino.

6. (Opcional) Para adicionar outra sub-rede de destino, escolha Add additional subnet (Adicionar sub-rede adicional) e faça o seguinte:

   - Em Middlebox, escolha o ID da interface de rede associado ao dispositivo middlebox ou, ao usar um endpoint de balanceador de carga do gateway, escolha o ID do endpoint da VPC.

     Você deve usar o mesmo dispositivo middlebox para várias sub-redes.
   - Em Destination subnet (Sub-rede de destino), escolha a sub-rede de destino.

7. (Opcional) Para adicionar outra origem, escolha Add source (Adicionar origem) e repita as etapas anteriores.
8. Escolha Próximo.
9. Na página Review and create (Revisar e criar), verifique as rotas e escolha Create routes (Criar rotas).

2. Modificar rotas do middlebox

Você pode editar sua configuração de rota alterando o gateway, o middlebox ou a sub-rede de destino.

Quando você faz alguma modificação, o assistente de roteamento do middlebox executa automaticamente as seguintes operações:

- Cria novas tabelas de rotas para o gateway, middlebox e sub-rede de destino.
- Adiciona as rotas necessárias às novas tabelas de rotas.
- Desassocia as tabelas de rotas atuais associadas pelo assistente de roteamento do middlebox aos recursos.
- Associa as novas tabelas de rotas criadas pelo assistente de roteamento do middlebox aos recursos.

Para modificar rotas do moddlebox usando o assistente de roteamento do middlebox

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.

2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Selecione sua VPC e escolha Actions (Ações), Manage middlebox routes (Gerenciar rotas do middlebox).
4. Escolha Edit routes (Editar rotas).
5. Para alterar o gateway, em Source (Origem), escolha o gateway por meio do qual o tráfego entra em sua VPC. Se você escolher um gateway privado virtual, insira o CIDR da sub-rede de destino em Destination IPv4 CIDR (CIDR IPv4 de destino).
6. Para adicionar outra sub-rede de destino, escolha Add additional subnet (Adicionar sub-rede adicional) e faça o seguinte:

   - Em Middlebox, escolha o ID da interface de rede associado ao dispositivo middlebox ou, ao usar um endpoint de balanceador de carga do gateway, escolha o ID do endpoint da VPC.

     Você deve usar o mesmo dispositivo middlebox para várias sub-redes.
   - Em Destination subnet (Sub-rede de destino), escolha a sub-rede de destino.
7. Escolha Próximo.
8. Na página Review and update (Revisar e atualizar), uma lista de tabelas de rotas e suas rotas que serão criadas pelo assistente de roteamento do middlebox será exibida. Verifique as rotas e, na caixa de diálogo de confirmação, escolha Update routes (Atualizar rotas).

3. Excluir a configuração do assistente de roteamento do middlebox

Se você decidir que não deseja mais a configuração do assistente de roteamento do middlebox, será necessário excluir manualmente as tabelas de rotas.

Para excluir a configuração do assistente de roteamento do middlebox

1. Visualizar as tabelas de rotas do assistente de roteamento do middlebox.

   Após a execução da operação, as tabelas de rotas criadas pelo assistente de roteamento do middlebox são exibidas em uma página separada da tabela de rotas.
2. Exclua cada tabela de rota exibida.

Considerações do assistente de roteamento do middleboxo

Leve o seguinte em consideração ao usar o assistente de roteamento do middlebox:

- Se desejar inspecionar o tráfego, use um gateway da Internet ou um gateway privado virtual como origem.
- Se você usar o mesmo middlebox em uma configuração de vários middlebox dentro da mesma VPC, verifique se o middlebox está na mesma posição de salto para ambas as sub-redes.
- O dispositivo deve ser configurado em uma sub-rede separada para a sub-rede de origem ou de destino.
- Você deve desabilitar a verificação de origem/destino no dispositivo. Para obter mais informações, consulte Alterar a verificação da origem ou destino no Guia do usuário do Amazon EC2.
- As tabelas de rotas e rotas criadas pelo assistente de roteamento do middlebox são contabilizadas em suas cotas. Para ter mais informações, consulte the section called “Tabelas de rotas”.
- Se você excluir um recurso, por exemplo uma interface de rede, as associações da tabela de rotas com o recurso serão removidas. Se o recurso for um destino, o destino da rota será definido como um “buraco negro”. As tabelas de rota não são excluídas.
- A sub-rede do middlebox e a sub-rede de destino devem ser associadas a uma tabela de rotas não padrão.

> **Note**
>
> Recomendamos usar o assistente de roteamento do middlebox para modificar ou excluir as tabelas de rotas criadas usando o assistente de roteamento do middlebox.

Cenários de middlebox

A Amazon Virtual Private Cloud (VPC) fornece uma ampla variedade de recursos de rede que permitem que você personalize e controle o roteamento do tráfego em sua rede virtual. Um desses recursos é o assistente de roteamento de middlebox, que possibilita o controle refinado do caminho de roteamento do tráfego que entra ou sai da VPC.

Se você precisar redirecionar o tráfego para um dispositivo de segurança, balanceador de carga ou outro dispositivo de rede para fins de inspeção, monitoramento ou otimização, o assistente de roteamento de middlebox pode simplificar o processo. Esse assistente cria automaticamente as tabelas de rotas e as rotas (saltos) necessárias para redirecionar o tráfego especificado conforme necessário, eliminando o esforço manual necessário para configurar configurações de roteamento complexas.

O assistente de roteamento de middlebox oferece suporte a vários cenários diferentes. Por exemplo, você pode usá-lo para inspecionar o tráfego destinado a uma sub-rede específica, configurar o roteamento e a inspeção do tráfego de middlebox em toda a sua VPC ou inspecionar seletivamente o tráfego entre sub-redes específicas. Esse controle granular sobre o roteamento de tráfego permite implementar políticas de segurança avançadas, torna possível o monitoramento centralizado da rede ou otimiza a performance de aplicações baseadas em nuvem.

Os exemplos a seguir descrevem cenários para o assistente de roteamento de middlebox.

Conteúdo

Inspecionar o tráfego destinado a uma sub-rede

Considere o cenário em que há tráfego entrando na VPC por meio de um gateway da Internet e você deseja inspecionar todo o tráfego destinado a uma sub-rede, digamos, sub-rede B, usando um dispositivo de firewall instalado em uma instância do EC2. O dispositivo de firewall deve ser instalado e configurado em uma instância do EC2 em uma sub-rede separada da sub-rede B na VPC, por exemplo, a sub-rede C. Você pode usar o assistente de roteamento do middlebox para configurar rotas para o tráfego entre a sub-rede B e o gateway da Internet.

O assistente de roteamento do middlebox executa automaticamente as seguintes operações:

- Cria as seguintes tabela de rotas:
  - Uma tabela de rotas para o gateway da Internet
  - Uma tabela de rotas para a sub-rede de destino
  - Uma tabela de rotas para a sub-rede do middlebox
- Adiciona as rotas necessárias às novas tabelas de rotas, conforme descrito nas seções a seguir.
- Desassocia as tabelas de rotas atuais associadas ao gateway da Internet, à sub-rede B e à sub-rede C.
- Associa a tabela de rotas A ao gateway da Internet (a fonte no assistente de roteamento do middlebox), à tabela de rotas C (o middlebox no assistente de roteamento do middlebox) e à tabela de rotas B com a sub-rede B (o destino no assistente de roteamento do middlebox).

- Cria uma tag que indica que ela foi criada pelo assistente de roteamento do middlebox e uma tag que indica a data de criação.

O assistente de roteamento do middlebox não modifica as tabelas de rotsa existentes. Ele cria novas tabelas de rotas e, em seguida, associa-as aos seus recursos de gateway e sub-rede. Se os recursos já estiverem explicitamente associados às tabelas de rotas existentes, as tabelas de rotas existentes serão primeiro desassociadas e, em seguida, as novas tabelas de rotas serão associadas aos seus recursos. Suas tabelas de rotas existentes não são excluídas.

Se você não usar o assistente de roteamento de middlebox, será necessário configurar manualmente e, em seguida, atribuir as tabelas de rota às sub-redes e ao gateway da Internet.

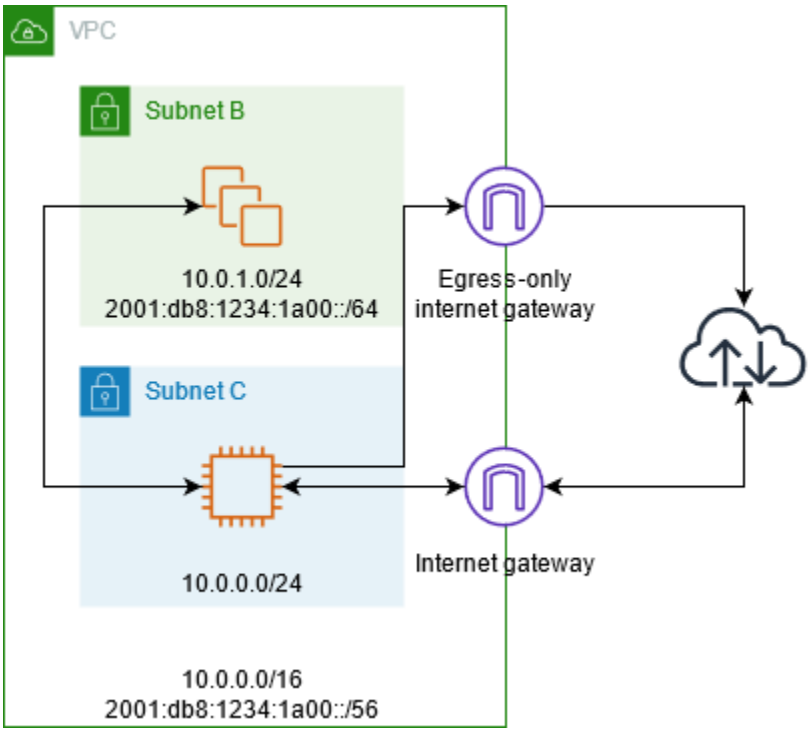


Tabela de rotas do gateway da Internet

Adicione as tabelas de rotas a seguir à tabela de rotas para o gateway da Internet.

Destino	Alvo	Finalidade
10.0.0.0/16	Local	Rota local para IPv4
10.0.1.0/24	*appliance-eni*	Rotear tráfego IPv4 destinado à sub-rede B para o middlebox

Destino	Alvo	Finalidade
2001:db8:1234:1a00::/56	Local	Rota local para IPv6
2001:db8:1234:1a00::/64	*appliance-eni*	Rotear tráfego IPv6 destinado à sub-rede B para o middlebox

Há uma associação de borda entre o gateway da Internet e a VPC.

Quando você usa o assistente de roteamento de middlebox, as seguintes tags são associadas à tabela de rotas:

- A chave é “Origin” e o valor é “Middlebox wizard”
- A chave é “date_created” (data da criação) e o valor é a hora de criação (por exemplo, “2021-02-18T22:25:49.137Z”)

Tabela de rotas da sub-rede de destino

Adicione as seguintes rotas à tabela de rotas para a sub-rede de destino (sub-rede B no diagrama de exemplo).

Destino	Alvo	Finalidade
10.0.0.0/16	Local	Rota local para IPv4
0.0.0.0/0	*appliance-eni*	Rotear tráfego IPv4 destinado à Internet para o middlebox
2001:db8:1234:1a00::/56	Local	Rota local para IPv6
::/0	*appliance-eni*	Encaminhar o tráfego IPv6 destinado à Internet para o middlebox

Há uma associação de sub-rede com a sub-rede do middlebox.

Quando você usa o assistente de roteamento de middlebox, as seguintes tags são associadas à tabela de rotas:

- A chave é “Origin” e o valor é “Middlebox wizard”
- A chave é “date_created” (data da criação) e o valor é a hora de criação (por exemplo, “2021-02-18T22:25:49.137Z”)

Tabela de rotas da sub-rede do middlebox

Adicione as seguintes rotas à tabela de rotas para a sub-rede do middlebox (sub-rede C no diagrama de exemplo).

Destino	Alvo	Finalidade
10.0.0.0/16	Local	Rota local para IPv4
0.0.0.0/0	*igw-id*	Rotear o tráfego IPv4 para o gateway da Internet
2001:db8:1234:1a00::/56	Local	Rota local para IPv6
::/0	*eigw-id*	Encaminhar o tráfego IPv6 para o gateway da Internet somente de saída

Há uma associação de sub-rede com a sub-rede de destino.

Quando você usa o assistente de roteamento de middlebox, as seguintes tags são associadas à tabela de rotas:

- A chave é “Origin” e o valor é “Middlebox wizard”
- A chave é “date_created” (data da criação) e o valor é a hora de criação (por exemplo, “2021-02-18T22:25:49.137Z”)

Configurar o roteamento e a inspeção de tráfego de middlebox em uma VPC

Considere o cenário em que você precisa inspecionar o tráfego que entra em uma VPC a partir do gateway da Internet e que é destinado a uma sub-rede, usando uma frota de dispositivos de

segurança configurados de forma subjacente a um Gateway Load Balancer. O proprietário da VPC do consumidor de serviço cria um endpoint do balanceador de carga do gateway em uma sub-rede na VPC (representada por uma interface de rede de endpoint). Todo o tráfego que entra na VPC através do gateway da Internet é encaminhado primeiro para o endpoint do balanceador de carga de gateway para inspeção antes de ser encaminhado para a sub-rede de destino. Da mesma forma, todo o tráfego que sai da sub-rede do aplicativo é roteado primeiro para o endpoint do balanceador de carga de gateway para inspeção antes de ser encaminhado para a Internet.

O assistente de roteamento para middlebox realiza automaticamente as seguintes operações:

- Cria as tabelas de rotas.
- Adiciona as rotas necessárias às novas tabelas de rotas.
- Desassocia as tabelas de rotas atuais associadas às sub-redes.
- Associa as tabelas de rotas criadas pelo assistente de roteamento do middlebox às sub-redes.
- Cria uma tag que indica que ela foi criada pelo assistente de roteamento do middlebox e uma tag que indica a data de criação.

O assistente de roteamento do middlebox não modifica as tabelas de rotsa existentes. Ele cria novas tabelas de rotas e, em seguida, associa-as aos seus recursos de gateway e sub-rede. Se os recursos já estiverem explicitamente associados às tabelas de rotas existentes, as tabelas de rotas existentes serão primeiro desassociadas e, em seguida, as novas tabelas de rotas serão associadas aos seus recursos. Suas tabelas de rotas existentes não são excluídas.

Se você não usar o assistente de roteamento de middlebox, será necessário configurar manualmente e, em seguida, atribuir as tabelas de rota às sub-redes e ao gateway da Internet.

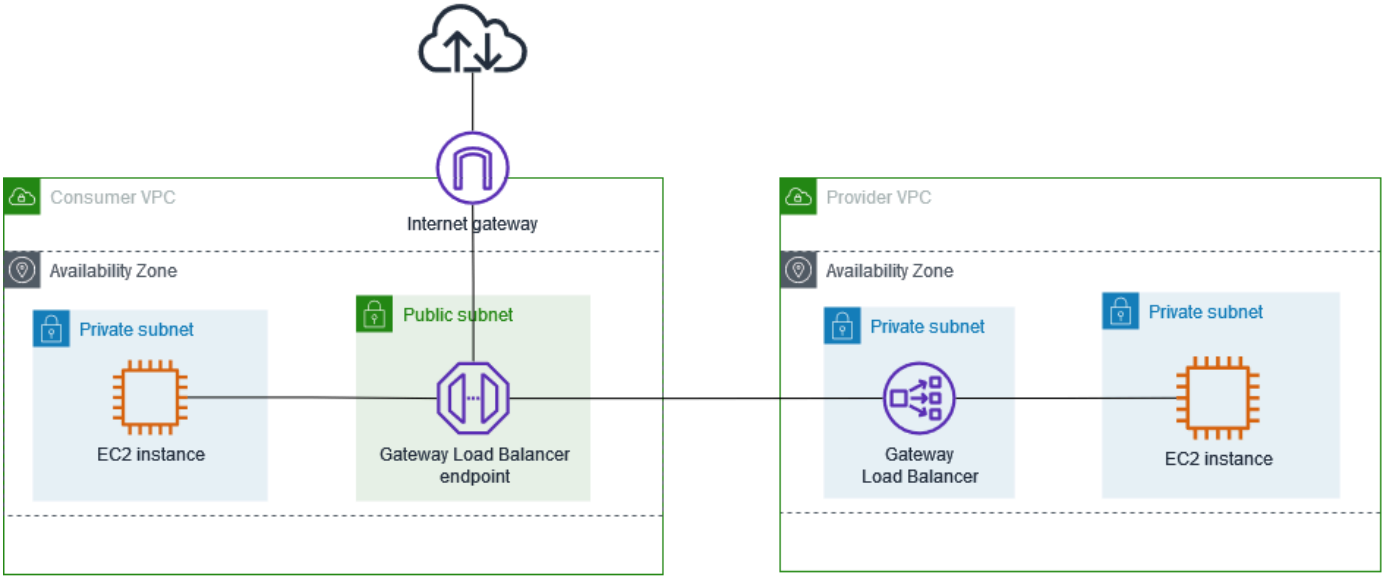


Tabela de rotas do gateway da Internet

A tabela de rotas do gateway da Internet contém as seguintes rotas:

Destino	Alvo	Finalidade
CIDR da VPC de consumo	Local	Rota local
CIDR da sub-rede do aplicativo	*endpoint-id*	Rotear o tráfego com destino à sub-rede da aplicação para o endpoint do Gateway Load Balancer

Há uma associação de borda com o gateway.

Quando você usa o assistente de roteamento de middlebox, as seguintes tags são associadas à tabela de rotas:

- A chave é “Origin” e o valor é “Middlebox wizard”
- A chave é “date_created” (data da criação) e o valor é a hora de criação (por exemplo, “2021-02-18T22:25:49.137Z”)

Tabela de rotas da sub-rede do aplicativo

A tabela de rotas para a sub-rede do aplicativo contém as seguintes rotas:

Destino	Alvo	Finalidade
CIDR da VPC de consumo	Local	Rota local
0.0.0.0/0	*endpoint-id*	Rotear o tráfego dos servidores da aplicação para o endpoint do Gateway Load Balancer antes que ele seja direcionado para a Internet

Quando você usa o assistente de roteamento de middlebox, as seguintes tags são associadas à tabela de rotas:

- A chave é “Origin” e o valor é “Middlebox wizard”
- A chave é “date_created” (data da criação) e o valor é a hora de criação (por exemplo, “2021-02-18T22:25:49.137Z”)

Tabela de rotas da sub-rede do provedor

A tabela de rotas para a sub-rede do provedor contém as seguintes rotas:

Destino	Alvo	Finalidade
CIDR da VPC do provedor	Local	Rota local. Garantir que o tráfego proveniente da Internet seja direcionado para os servidores de aplicação
0.0.0.0/0	*igw-id*	Roteia todo o tráfego para o gateway da Internet

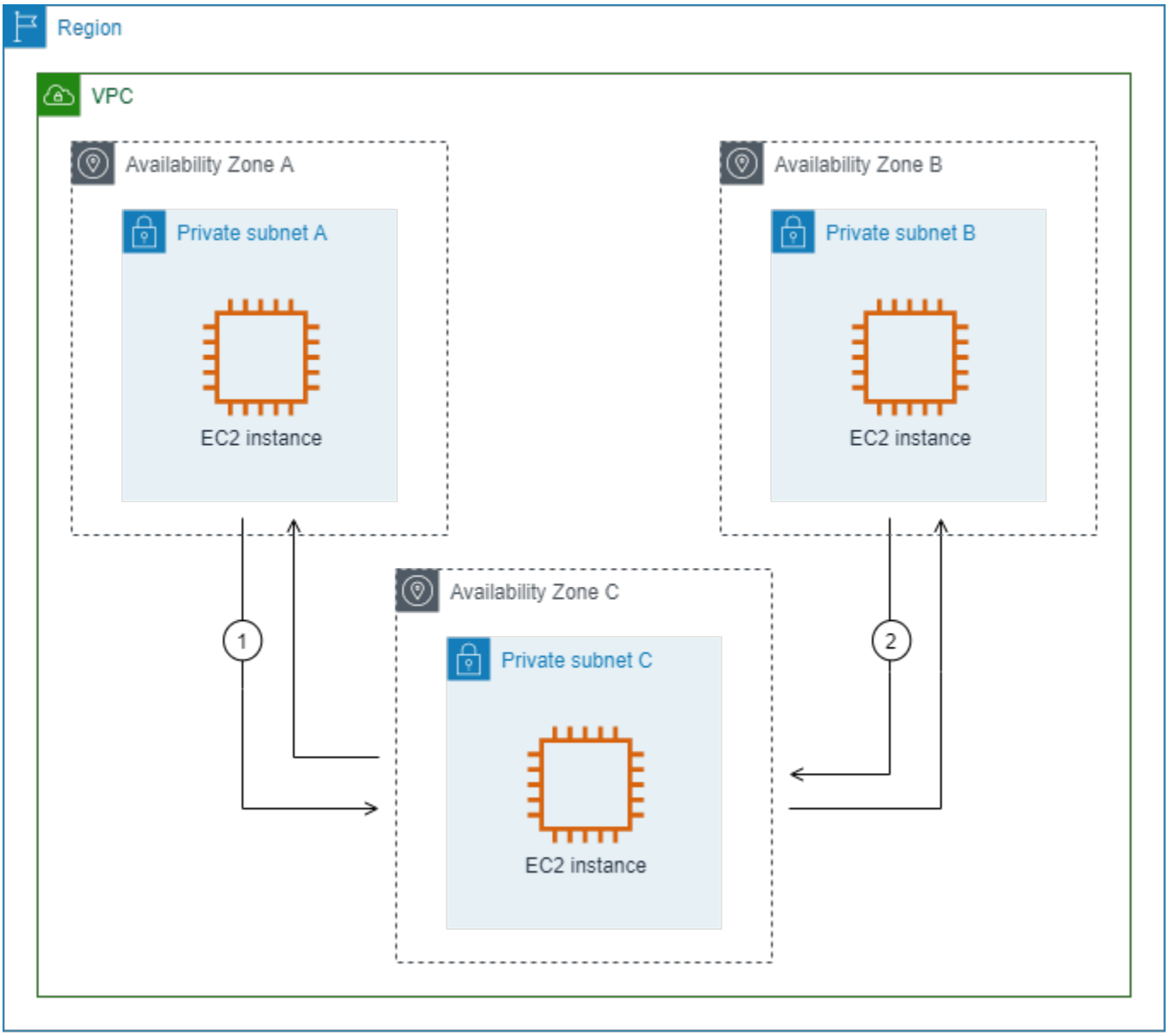
Quando você usa o assistente de roteamento de middlebox, as seguintes tags são associadas à tabela de rotas:

- A chave é “Origin” e o valor é “Middlebox wizard”
- A chave é “date_created” (data da criação) e o valor é a hora de criação (por exemplo, “2021-02-18T22:25:49.137Z”)

Inspecionar o tráfego entre sub-redes

Considere o cenário em que você tem várias sub-redes em uma VPC e deseja inspecionar o tráfego entre elas usando um dispositivo de firewall. Configure e instale o dispositivo de firewall em uma instância do EC2 em uma sub-rede diferente em sua VPC.

O diagrama a seguir mostra um dispositivo de firewall instalado em uma instância do EC2 na sub-rede C. O dispostivo inspeciona todo o tráfego que passa da sub-rede A para a sub-rede B (consulte 1) e da sub-rede B para a sub-rede A (consulte 2).



Você usa a tabela de rotas principal para a VPC e a sub-rede do middlebox. As sub-redes A e B têm uma tabela de rotas personalizada cada.

O assistente de roteamento do middlebox executa automaticamente as seguintes operações:

- Cria as tabelas de rotas.
- Adiciona as rotas necessárias às novas tabelas de rotas.
- Desassocia as tabelas de rotas atuais associadas às sub-redes.
- Associa as tabelas de rotas criadas pelo assistente de roteamento do middlebox às sub-redes.
- Cria uma tag que indica que ela foi criada pelo assistente de roteamento do middlebox e uma tag que indica a data de criação.

O assistente de roteamento do middlebox não modifica as tabelas de rotsa existentes. Ele cria novas tabelas de rotas e, em seguida, associa-as aos seus recursos de gateway e sub-rede. Se os recursos já estiverem explicitamente associados às tabelas de rotas existentes, as tabelas de rotas existentes serão primeiro desassociadas e, em seguida, as novas tabelas de rotas serão associadas aos seus recursos. Suas tabelas de rotas existentes não são excluídas.

Se você não usar o assistente de roteamento de middlebox, será necessário configurar manualmente e, em seguida, atribuir as tabelas de rota às sub-redes e ao gateway da Internet.

Tabela de rotas personalizada da sub-rede A

A tabela de rotas para a sub-rede A contém as seguintes rotas:

Destino	Alvo	Finalidade
CIDR DA VPC	Local	Rota local
CIDR da sub-rede B	*appliance-eni*	Rotear tráfego destinado à sub-rede B para o middlebox

Quando você usa o assistente de roteamento de middlebox, as seguintes tags são associadas à tabela de rotas:

- A chave é “Origin” e o valor é “Middlebox wizard”
- A chave é “date_created” (data da criação) e o valor é a hora de criação (por exemplo, “2021-02-18T22:25:49.137Z”)

Tabela de rotas personalizada da sub-rede B

A tabela de rotas para a sub-rede B contém as seguintes rotas.

Destino	Alvo	Finalidade
CIDR DA VPC	Local	Rota local
CIDR da sub-rede A	*appliance-eni*	Rotear tráfego destinado à sub-rede A para o middlebox

Quando você usa o assistente de roteamento de middlebox, as seguintes tags são associadas à tabela de rotas:

- A chave é “Origin” e o valor é “Middlebox wizard”
- A chave é “date_created” (data da criação) e o valor é a hora de criação (por exemplo, “2021-02-18T22:25:49.137Z”)

Tabela de rotas principal

A sub-rede C usa a tabela de rotas principal. A tabela de rotas principal contém as rotas a seguir.

Destino	Alvo	Finalidade
CIDR DA VPC	Local	Rota local

Quando você usa o assistente de roteamento de middlebox, as seguintes tags são associadas à tabela de rotas:

- A chave é “Origin” e o valor é “Middlebox wizard”
- A chave é “date_created” (data da criação) e o valor é a hora de criação (por exemplo, “2021-02-18T22:25:49.137Z”)

Excluir uma sub-rede

Se não precisar mais de uma sub-rede, é possível excluí-la. Você não poderá excluir uma sub-rede se ela contiver qualquer interface de rede. Por exemplo, é necessário terminar todas as instâncias em uma sub-rede antes de excluí-la.

Quando você exclui uma sub-rede, o bloco CIDR associado a essa sub-rede é retornado ao pool de endereços IP disponíveis da VPC. Isso significa que os endereços IP dentro do intervalo CIDR da sub-rede podem ser realocados para outras sub-redes ou recursos dentro da mesma VPC.

É importante observar que a exclusão de uma sub-rede não exclui automaticamente os recursos que fazem parte dela. Primeiro, é necessário encerrar todas as instâncias do EC2, excluir todas as interfaces de rede e remover quaisquer outros recursos associados à sub-rede antes de continuar com a exclusão da sub-rede.

Para excluir uma sub-rede usando o console

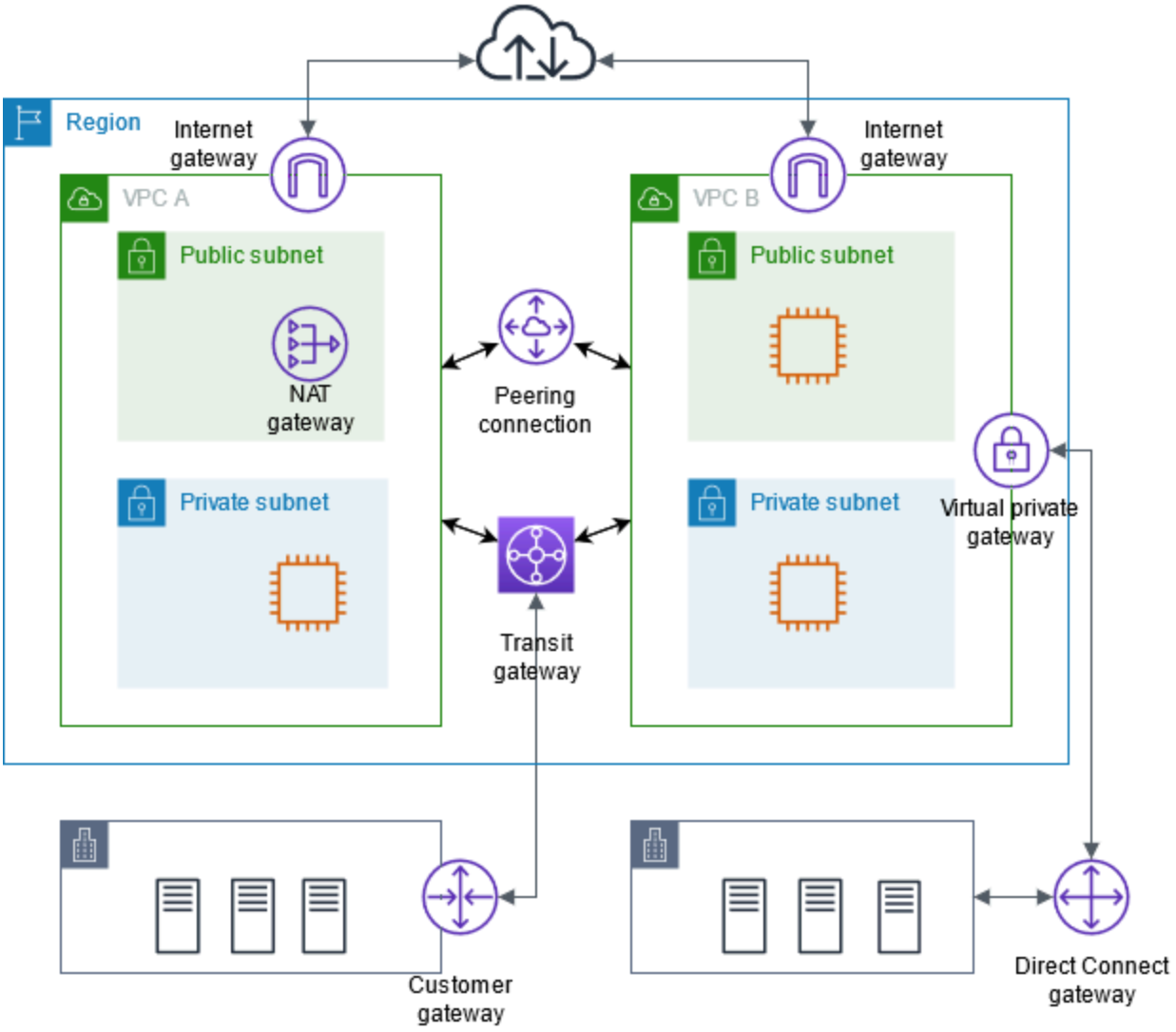
1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Termine todas as instâncias na sub-rede. Para obter mais informações, consulte Terminar sua instância no Guia do usuário do Amazon EC2.
3. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
4. No painel de navegação, escolha Sub-redes.
5. Selecione a sub-rede e escolha Actions (Ações), Delete subnet (Excluir sub-rede).
6. Quando a confirmação for solicitada, insira **`delete`** e escolha Delete (Excluir).

Para excluir uma sub-rede usando a AWS CLI

Use o comando delete-subnet.

Conectar sua VPC a outras redes

É possível conectar sua VPC a outras redes, como outras VPCs, a Internet ou uma rede on-premises própria.



É possível conectar sua VPC a outras redes, como outras VPCs, a Internet ou uma rede on-premises própria.

O diagrama a seguir demonstra algumas dessas opções de conectividade. A VPC A está conectada à Internet por meio de um gateway da Internet, e a instância do EC2 na sub-rede privada pode se conectar à Internet usando um gateway NAT na sub-rede pública. A VPC B também está conectada à Internet, mas por meio de um gateway da Internet direto, permitindo que a instância do EC2 na sub-rede pública acesse a Internet.

Mais ainda, VPC A e VPC B estão conectadas entre si por meio de uma conexão de emparelhamento de VPC e de um gateway de trânsito. O gateway de trânsito tem um anexo da VPN para um data center, e VPC B tem uma conexão AWS Direct Connect para o mesmo data center. Essa interconectividade permite que as organizações integrem seus recursos de nuvem à infraestrutura on-premises, criando um ambiente de nuvem híbrida.

Conectar VPCs a outras redes é um aspecto importante da criação de uma infraestrutura de nuvem na AWS. Fazer isso oferece às organizações flexibilidade e controle sobre suas configurações de rede, permitindo que elas projetem arquiteturas de VPC que se alinhem aos requisitos de negócios e às necessidades de segurança. Essas opções de conectividade facilitam o fluxo eficiente de dados entre vários componentes de um cenário de TI distribuído, estejam eles na nuvem ou on-premises.

A AWS fornece toda uma variedade de ferramentas e recursos para habilitar essas conexões VPC, incluindo gateways de internet, gateways NAT, emparelhamento de VPC, gateways de trânsito e o AWS Direct Connect. Ao empregar esses recursos, as organizações podem criar ambientes de nuvem seguros e perfeitamente integrados à infraestrutura de TI existente.

Você pode conectar sua nuvem privada virtual (VPC) a outras redes. Por exemplo, outras VPCs, a Internet ou uma rede on-premises própria.

Para mais informações, consulte as Amazon Virtual Private Cloud Connectivity Options (Opções de conectividade da Amazon Virtual Private Cloud).

Conteúdo

Habilitar o acesso da VPC à Internet usando gateways da Internet

Um gateway da Internet é um componente da VPC horizontalmente dimensionado, redundante e altamente disponível que permite a comunicação entre a VPC e a Internet. Ele oferece suporte para

tráfego IPv4 e IPv6. Não causa riscos de disponibilidade ou restrições de largura de banda no tráfego de rede.

Um gateway da Internet habilita recursos em suas sub-redes públicas (como instâncias do EC2) para estabelecer conexão com a Internet se o recurso tiver um endereço IPv4 ou um endereço IPv6 público. Da mesma forma, os recursos na Internet podem iniciar uma conexão com recursos em sua sub-rede usando o endereço IPv4 ou o endereço IPv6 público. Por exemplo, um gateway da Internet permite que você estabeleça conexão com uma instância do EC2 na AWS usando seu computador local.

Um gateway da Internet fornece um destino nas tabelas de rotas da VPC para tráfego roteável pela Internet. Para a comunicação usando o IPv4, o gateway da Internet também executa a conversão de endereços de rede (NAT). Para obter mais informações, consulte Endereços IP e NAT.

> **Note**
>
> Não há cobrança por um gateway da Internet, mas há cobranças para a transferência de dados para instâncias EC2 que usam gateways da Internet. Para mais informações, consulte Amazon EC2 On-Demand Pricing (Preços do Amazon EC2 sob demanda).

Conteúdo

Configuração para acesso à Internet

Para permitir que as instâncias recebam ou enviem tráfego da Internet, faça o seguinte:

- Crie um gateway da internet e anexe-o à sua VPC.
- Adicione uma rota à tabela de rotas da sub-rede que direciona o tráfego de entrada da internet para o gateway da Internet.
- Certifique-se de que as instâncias na sub-rede tenham um endereço IPv4 ou endereços IPv6 públicos. Para obter mais informações, consulte a seção Endereçamento IP de instâncias no Guia do Usuário do Amazon EC2.
- Garanta que seus grupos de segurança e listas de controle de acesso à rede permitam a passagem do tráfego desejado da Internet para suas instâncias e vice-versa.

Caso deseje proporcionar acesso à internet para suas instâncias sem atribuir a elas endereços IP públicos, empregue um dispositivo NAT. Um dispositivo NAT permite que instâncias em uma sub-rede privada se conectem à Internet, mas impede que os hosts na Internet iniciem conexões com as instâncias. Para ter mais informações, consulte Dispositivos NAT.

Sub-redes públicas e privadas

Se uma sub-rede estiver associada a uma tabela de rotas que tem uma rota para um gateway da Internet, ela é conhecida como sub-rede pública. Se uma sub-rede estiver associada a uma tabela de rotas que não tem uma rota para um gateway da Internet, ela é conhecida como sub-rede privada.

Na tabela de rotas da sub-rede pública, é possível especificar uma rota para o gateway da Internet para todos os destinos não explicitamente conhecidos pela tabela de rotas (`0.0.0.0/0` para IPv4 ou `::/0` para IPv6). Como alternativa, avalie a rota para uma faixa menor de endereços IP, por exemplo, os endereços IPv4 públicos dos endpoints públicos da empresa fora da AWS, ou os endereços IP elásticos de outras instâncias do Amazon EC2 fora da VPC.

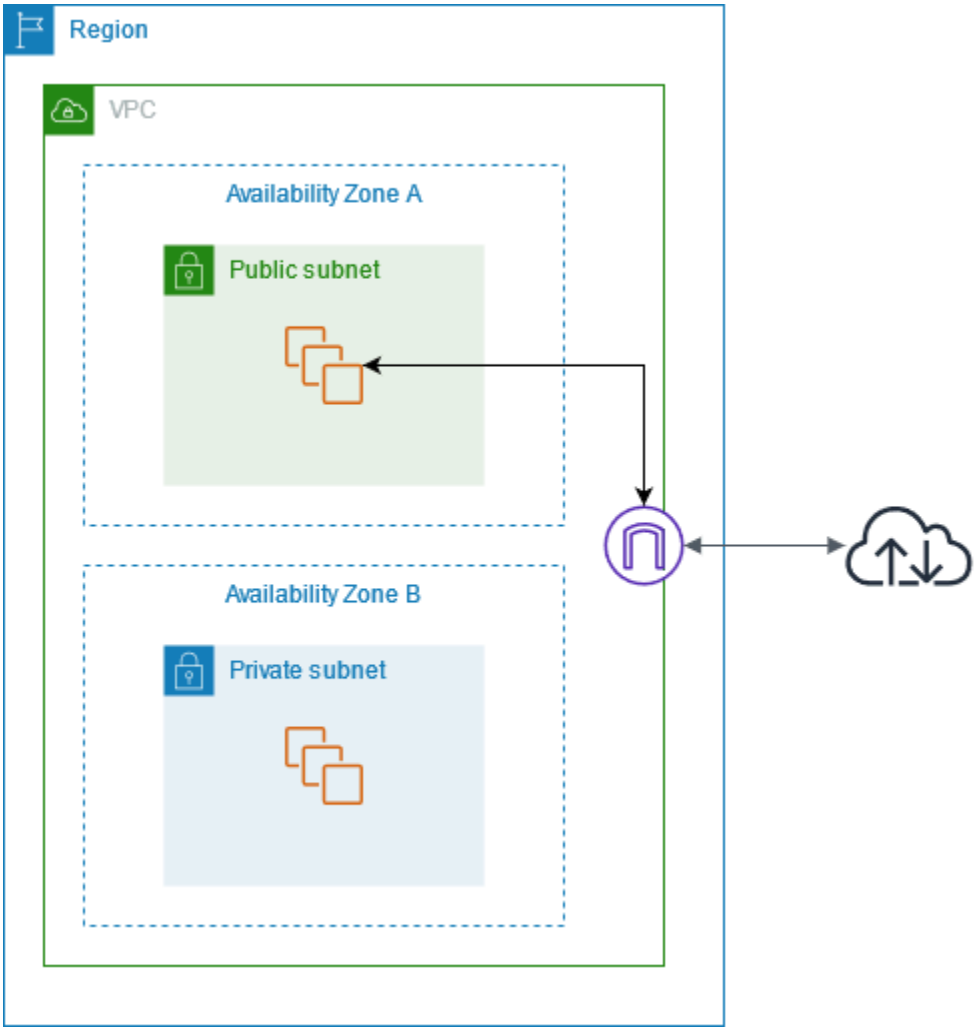
Endereços IP e NAT

Para permitir a comunicação pela internet para o IPv4, a instância deve ter um endereço IPv4 público. Você pode configurar a VPC para atribuir automaticamente endereços IPv4 públicos às instâncias ou pode atribuir endereços IP elásticos às instâncias. A instância detém a informação apenas do espaço de endereço IP privado (interno) definido na VPC e na sub-rede. O gateway da internet fornece logicamente o NAT individualizado em nome da instância, de modo que, quando o tráfego deixa a sub-rede da VPC e vai para a internet, o campo do endereço de resposta é definido como o endereço IPv4 público ou o endereço IP elástico da instância, e não como o endereço IP privado. Por outro lado, o tráfego destinado ao endereço IPv4 público ou ao endereço IP elástico da instância tem seu endereço de destino traduzido para o endereço IPv4 privado da instância antes do tráfego ser entregue à VPC.

Para permitir a comunicação pela internet para IPv6, a VPC e a sub-rede devem ter um bloco CIDR IPv6 associado, além de ser atribuído à instância um endereço IPv6 no intervalo da sub-rede. Os endereços IPv6 são exclusivos globalmente e, portanto, públicos por padrão.

No diagrama a seguir, a sub-rede na zona de disponibilidade é uma sub-rede pública. A tabela de rotas desta sub-rede tem uma rota que envia todo o tráfego IPv4 vinculado à Internet para o gateway da Internet. As instâncias na sub-rede pública devem ter endereços IP públicos ou endereços de IP elásticos para permitir a comunicação com a Internet pelo gateway da Internet. Para comparação, a sub-rede na Zona de disponibilidade B é uma sub-rede privada porque sua tabela de rotas não tem

uma rota para o gateway da Internet. Como não há rota para o gateway da Internet, as instâncias na sub-rede privada não podem se comunicar com a Internet mesmo que tenham endereços IP públicos.



Acesso à Internet para VPCs padrão e não padrão

A tabela a seguir fornece uma visão geral para identificar se a VPC já possui os componentes necessários para acesso à Internet por meio de IPv4 ou IPv6.

Componente	VPC padrão	VPC não padrão
Gateway da Internet	Sim	Não
Tabela de rotas com rota para o gateway da internet para tráfego IPv4 (0.0.0.0/0)	Sim	Não

Componente	VPC padrão	VPC não padrão
Tabela de rotas com rota para o gateway da internet para tráfego IPv6 (::/0)	Não	Não
Endereço IPv4 público atribuído automaticamente à instância executada na sub-rede	Sim (sub-rede padrão)	Não (sub-rede não padrão)
Endereço IPv6 atribuído automaticamente à instância executada na sub-rede	Não (sub-rede padrão)	Não (sub-rede não padrão)

Para obter mais informações sobre VPCs padrão, consulte VPCs padrão. Para obter mais informações sobre a criação de uma VPC, consulte Crie uma VPC.

Adicionar acesso à Internet a uma sub-rede

As seções a seguir descrevem como oferecer suporte ao acesso à Internet em uma sub-rede na VPC usando um gateway da Internet. Para remover o acesso à Internet, você pode desvincular o gateway da Internet da sua VPC e depois excluí-lo.

Tarefas

- 1. Criar um gateway da internet
- 2. Anexar ou desanexar um gateway da Internet de uma VPC
- 3. Excluir um gateway da internet
- Visão geral da linha de comando

1. Criar um gateway da internet

Use o procedimento a seguir para criar um gateway da internet.

Para criar um gateway da Internet

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.

2. No painel de navegação, escolha Internet gateways (Gateways da Internet).
3. Escolha Criar gateway da Internet.
4. (Opcional) Insira um nome para o gateway da Internet.
5. (Opcional) Para adicionar uma tag, escolha Add new tag (Adicionar nova tag) e insira a chave e o valor da tag.
6. Escolha Criar gateway da Internet.
7. (Opcional) Para conectar o gateway da Internet a uma VPC agora, escolha Anexar a uma VPC no banner na parte superior da tela, selecione uma VPC disponível e escolha Anexar gateway da Internet. Caso contrário, você pode anexar o gateway da Internet a uma VPC em outro momento.

2. Anexar ou desanexar um gateway da Internet de uma VPC

Para usar um gateway da Internet, você deve anexá-lo a uma VPC.

Se não precisar mais de acesso à Internet para as instâncias executadas em uma VPC, você poderá desanexar um gateway da Internet de uma VPC. Você não poderá desanexar um gateway da internet se a VPC tiver recursos com endereços IP públicos ou endereços IP elásticos associados.

Para anexar ou desanexar um gateway da Internet de uma VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Internet gateways (Gateways da Internet).
3. Marque a caixa ao lado do gateway da Internet.
4. Para anexar, escolha Ações, Anexar à VPC, selecione uma VPC disponível e escolha Anexar gateway da Internet.
5. Para desanexar, escolha Ações, Desanexar da VPC e escolha Desanexar gateway da Internet. Quando a confirmação for solicitada, selecione Desanexar gateway da Internet.

3. Excluir um gateway da internet

Caso não precise mais de um gateway da internet, exclua-o. Você não pode excluir um gateway da internet se ele ainda estiver anexado a uma VPC.

Para excluir um gateway da internet

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Internet gateways (Gateways da Internet).
3. Marque a caixa ao lado do gateway da Internet.
4. Escolha Ações, Excluir gateway da Internet.
5. Quando a confirmação for solicitada, insira **`delete`** e escolha Excluir gateway da internet.

Visão geral da linha de comando

É possível executar as tarefas descritas nesta página por meio da linha de comando.

Criar um gateway da internet

- create-internet-gateway (AWS CLI)
- New-EC2InternetGateway (AWS Tools for Windows PowerShell)

Anexar um gateway da internet a uma VPC

- attach-internet-gateway (AWS CLI)
- Add-EC2InternetGateway (AWS Tools for Windows PowerShell)

Descrever um gateway da internet

- describe-internet-gateways (AWS CLI)
- Get-EC2InternetGateway (AWS Tools for Windows PowerShell)

Desanexar um gateway da Internet de uma VPC

- detach-internet-gateway (AWS CLI)
- Dismount-EC2InternetGateway (AWS Tools for Windows PowerShell)

Excluir um gateway da internet

- delete-internet-gateway (AWS CLI)
- Remove-EC2InternetGateway (AWS Tools for Windows PowerShell)

Habilitar o tráfego IPv6 de saída usando gateways da Internet somente de saída

Um gateway da Internet somente de saída é um componente da VPC horizontalmente escalado, redundante e altamente disponível que permite a comunicação de saída pela IPv6 das instâncias na VPC para a Internet e impede a Internet de iniciar uma conexão IPv6 com suas instâncias.

Um gateway da Internet somente de saída deve ser usado apenas com tráfego IPv6. Para habilitar a comunicação via Internet somente de saída pela IPv4, use um gateway NAT. Para ter mais informações, consulte Gateways NAT.

Preços

Não há cobrança por um gateway da Internet somente de saída, mas há cobranças para a transferência de dados para instâncias do EC2 que usam gateways da Internet. Para mais informações, consulte Amazon EC2 On-Demand Pricing (Preços do Amazon EC2 sob demanda).

Conteúdo

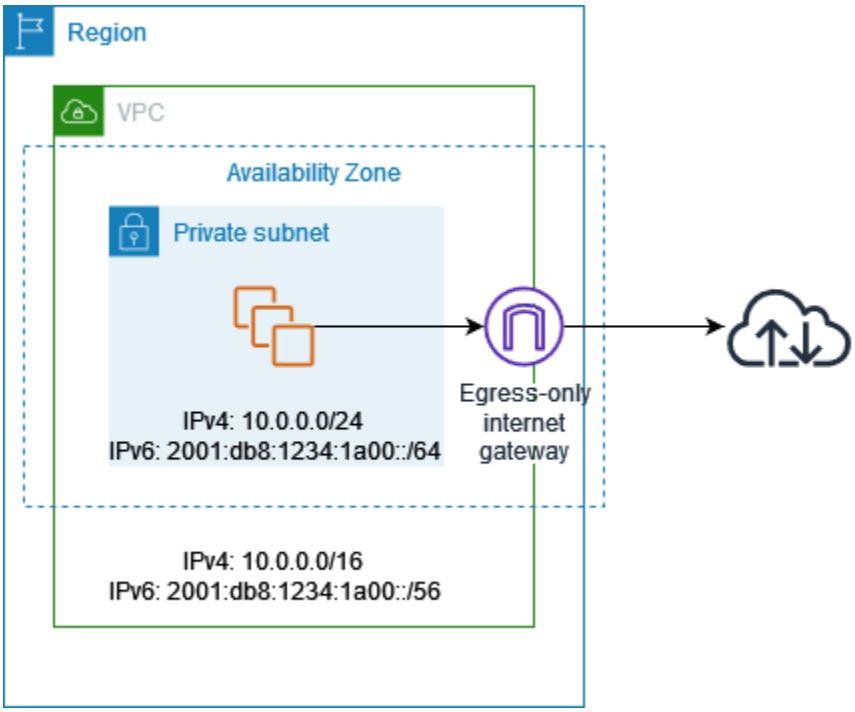
Noções básicas do Gateway da Internet somente de saída

Os endereços IPv6 são exclusivos globalmente e, são portanto, públicos por padrão. Se deseja que a instância possa acessar a Internet, mas deseja impedir que recursos na Internet iniciem a comunicação com a instância, será possível usar um gateway da Internet somente de saída. Para fazer isso, crie um gateway da Internet somente de saída na VPC e adicione uma rota à tabela de rotas que aponte todo o tráfego IPv6 (`::/0`) ou um intervalo específico de endereço IPv6 para o gateway da Internet somente de saída. O tráfego IPv6 na sub-rede associada à tabela de rotas é roteado para o gateway da Internet somente de saída.

Um gateway da Internet somente de saída é com estado: encaminha o tráfego das instâncias da sub-rede para a Internet ou outros serviços da AWS e envia a resposta de volta para as instâncias.

Você não pode associar um grupo de segurança a um gateway da internet somente de saída para controlar o tráfego que pode chegar ou sair do gateway da internet somente de saída. É possível usar um network ACL para controlar o tráfego de entrada e saída da sub-rede para a qual o gateway da Internet somente de saída roteia o tráfego.

No diagrama a seguir, a VPC tem blocos CIDR IPv4 e IPv6, e a sub-rede tem blocos CIDR IPv4 e IPv6. A VPC tem um gateway da Internet somente de saída.



A seguir apresentamos um exemplo da tabela de rotas associada à sub-rede. Há uma rota que envie todo o tráfego IPv6 (::/0) direcionado à Internet para o gateway da Internet apenas de saída.

Destino	Destino
10.0.0.0/16	Local
2001:db8:1234:1a00:/64	Local
::/0	*eigw-id*

Adicionar acesso à Internet apenas de saída a uma sub-rede

As tarefas a seguir descrevem como criar um gateway da Internet somente de saída para a sub-rede privada e configurar o roteamento da sub-rede.

Tarefas

- 1. Criar um gateway da Internet somente de saída
- 2. Criar uma tabela de rotas personalizada

- 3. Excluir um gateway da Internet somente de saída
- Visão geral da linha de comando

1. Criar um gateway da Internet somente de saída

É possível criar um gateway da Internet somente de saída para a VPC usando o console da Amazon VPC.

Como criar um gateway da Internet somente de saída para a VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Gateways da Internet somente de saída.
3. Selecione Criar um Gateway da Internet somente de saída.
4. (Opcional) Adicione ou remova uma tag.

   [Adicionar uma tag] Escolha Adicionar nova tag e faça o seguinte:

   - Em Chave, insira o nome da chave.
   - Em Value (Valor), insira o valor da chave.

   [Remover uma tag] Escolha Remover à direita da chave e do valor da tag.
5. Selecione a VPC para a qual será criado um gateway de Internet somente de saída.
6. Escolha Criar.

2. Criar uma tabela de rotas personalizada

Para enviar o tráfego destinado fora da VPC para o gateway da Internet somente de saída, é necessário criar uma tabela de rotas personalizada, adicionar uma rota que envia o tráfego para o gateway e associá-lo à sub-rede.

Como criar uma tabela de rotas personalizada e adicionar uma rota para o gateway da Internet somente de saída

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Route tables (Tabelas de rotas), Create route table (Criar tabela de rotas).

3. Na caixa de diálogo Create route table (Criar tabela de rotas), atribua um nome (opcional) à tabela de rotas e selecione a VPC e escolha Create route table (Criar tabela de rotas).
4. Selecione a tabela de rotas personalizada que acabou de ser criada. O painel de detalhes exibe as guias para trabalhar com as respectivas rotas, associações e propagação de rotas.
5. Na guia Routes (Rotas), escolha Edit routes (Editar rotas), especifique `::/0` na caixa Destination (Destino), selecione o ID do gateway da Internet na lista Target (Destino) e escolha Save changes (Salvar alterações).
6. Na guia Subnet associations (Associações de sub-rede), escolha Edit subnet associations (Editar) e marque a caixa de seleção para a sub-rede. Escolha Salvar.

Alternativamente, você pode adicionar uma rota a uma tabela de rotas existente associada à sua sub-rede. Selecione sua tabela de rotas existente e siga as etapas 5 e 6 acima para adicionar uma rota ao gateway da Internet somente de saída.

Para obter mais informações sobre tabelas de rotas, consulte Configurar tabelas de rotas.

3. Excluir um gateway da Internet somente de saída

Se você não precisar mais de um gateway da Internet somente de saída, é possível excluí-lo. Qualquer rota em uma tabela de rotas que aponta para o gateway da Internet somente de saída excluído permanece em um status `blackhole` até que você exclua ou atualize manualmente a rota.

Como excluir um gateway da Internet somente de saída

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Gateways da Internet somente de saída e selecione o gateway da Internet somente de saída.
3. Escolha Delete (Excluir).
4. Selecione Delete Egress Only Internet Gateway na caixa de diálogo de confirmação.

Visão geral da linha de comando

É possível executar as tarefas descritas nesta página por meio da linha de comando.

Criar um gateway da Internet somente de saída

- create-egress-only-internet-gateway (AWS CLI)

- New-EC2EgressOnlyInternetGateway (AWS Tools for Windows PowerShell)

Descrever um gateway da Internet somente de saída

- describe-egress-only-internet-gateways (AWS CLI)
- Get-EC2EgressOnlyInternetGatewayList (AWS Tools for Windows PowerShell)

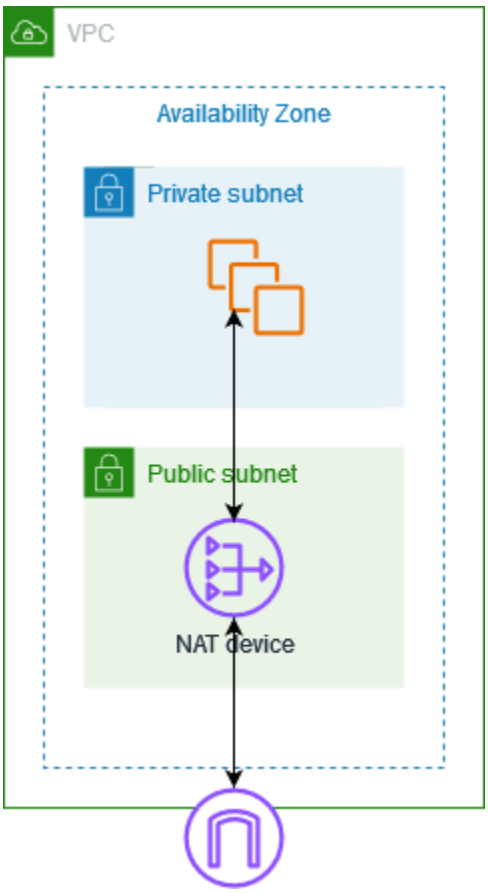
Excluir um gateway da Internet somente de saída

- delete-egress-only-internet-gateway (AWS CLI)
- Remove-EC2EgressOnlyInternetGateway (AWS Tools for Windows PowerShell)

Estabelecer conexão com a Internet ou a outras redes usando dispositivos NAT

Você pode usar um dispositivo NAT para permitir que recursos em sub-redes privadas se conectem à Internet, a outras VPCs ou a redes on-premises. Essas instâncias podem se comunicar com serviços fora da VPC, mas não podem receber solicitações de conexão não solicitadas.

Por exemplo, o diagrama a seguir mostra um dispositivo NAT em uma sub-rede pública que permite que as instâncias do EC2 em uma sub-rede privada se conectem à Internet por meio de um gateway da Internet. O dispositivo de NAT substitui o endereço IPv4 de origem das instâncias pelo endereço do dispositivo de NAT. Ao enviar tráfego de resposta para as instâncias, o dispositivo de NAT converte os endereços de volta para os endereços IPv4 de origem original.



Important

- Usamos o termo NAT nesta documentação para seguir a prática comum em TI, embora a função real de um dispositivo NAT seja conversão de endereços e port address translation (PAT – conversão de endereços de porta).
- Você pode usar um dispositivo de NAT gerenciado oferecido pela AWS chamado gateway NAT ou criar seu próprio dispositivo de NAT em uma instância do EC2, o que é chamado de instância de NAT. Recomendamos usar gateways NAT porque eles fornecem melhor disponibilidade e largura de banda e exigem menos esforço para administrar.

Conteúdo

Gateways NAT

Um gateway NAT é um serviço de Network Address Translation (NAT – Conversão de endereços de rede). Você pode usar um gateway NAT para que as instâncias em uma sub-rede privada possam se conectar a serviços fora da VPC, mas os serviços externos não podem iniciar uma conexão com essas instâncias.

Ao criar um gateway NAT, você deve especificar um dos seguintes tipos de conectividade:

- Public: (Padrão) instâncias em sub-redes privadas podem se conectar à Internet por meio de um gateway NAT público, mas não podem receber conexões de entrada não solicitadas da Internet. Você cria um gateway NAT público em uma sub-rede pública e deve associar um endereço IP elástico ao gateway NAT na criação. Encaminhe tráfego do gateway NAT para o gateway da Internet da VPC. Como alternativa, você pode usar um gateway NAT público para se conectar a outras VPCs ou à rede on-premises. Nesse caso, você roteia o tráfego do gateway NAT por meio de um gateway de trânsito ou de um gateway privado virtual.
- Private (Privado): instâncias em sub-redes privadas podem se conectar a outras VPCs ou à sua rede on-premises por meio de um gateway NAT privado. Você pode rotear o tráfego do gateway NAT por meio de um gateway de trânsito ou de um gateway privado virtual. Não é possível associar um endereço IP elástico a um gateway NAT privado. É possível associar um gateway da Internet a uma VPC com um gateway NAT privado, mas se você rotear o tráfego do gateway NAT privado para o gateway da Internet, o gateway da Internet descartará o tráfego.

Um gateway NAT deve ser usado com tráfego IPv4 ou IPv6 (via DNS64 e NAT64). Outra opção para habilitar a comunicação via Internet somente de saída via IPv6 é usar um gateway da Internet somente de saída.

Os gateways NAT privados e públicos mapeiam o endereço IPv4 privado de origem das instâncias para o endereço IPv4 privado do gateway NAT, mas no caso de um gateway NAT público, o gateway da Internet mapeia o endereço IPv4 privado do gateway NAT público para o endereço IP elástico associado ao gateway NAT. Ao enviar tráfego de resposta para as instâncias, seja um gateway NAT público ou privado, o gateway NAT converte o endereço de volta para o endereço IP de origem inicial.

> **Important**
>
> Você pode usar um gateway NAT público ou privado para rotear o tráfego para gateways de trânsito e gateways virtuais privados.

Se você usar um gateway NAT privado para se conectar a um gateway de trânsito ou a um gateway privado virtual, o tráfego para o destino virá do endereço IP privado do gateway NAT privado.
Se você usar um gateway NAT público para se conectar a um gateway de trânsito ou um gateway privado virtual, o tráfego para o destino virá do endereço IP privado do gateway NAT público. O gateway NAT público só usará seu EIP como endereço IP de origem quando for usado em conjunto com um gateway da Internet na mesma VPC.
Os gateways NAT oferecem suporte a tráfego com uma unidade de transmissão máxima (MTU) de 8500. Para ter mais informações, consulte Noções básicas de gateway NAT.

Conteúdo

Noções básicas de gateway NAT

Todo gateway NAT é criado em uma Zona de disponibilidade específica e implementado com redundância nessa zona. Há uma cota de gateways NAT que podem ser criados em cada zona de disponibilidade. Para obter mais informações, consulte Cotas da Amazon VPC.

Se você tiver recursos em várias zonas de disponibilidade e eles compartilharem um gateway NAT, caso a zona de disponibilidade do gateway NAT fique inativa, os recursos em outras zonas de disponibilidade perderão o acesso à Internet. Para melhorar a resiliência, crie um gateway NAT em cada zona de disponibilidade e configure seu roteamento para garantir que os recursos usem o gateway NAT na mesma zona de disponibilidade.

As seguintes características e regras se aplicam aos gateways NAT:

- Um gateway NAT é compatível com os seguintes protocolos: TCP, UDP e ICMP.

- Os gateways NAT são compatíveis com tráfego IPv4 ou IPv6. Para tráfego IPv6, o gateway NAT executa NAT64. Usando isso em conjunto com o DNS64 (disponível no Route 53 Resolver), suas workloads IPv6 em uma sub-rede na Amazon VPC podem se comunicar com recursos IPv4. Esses serviços IPv4 podem estar presentes na mesma VPC (em uma sub-rede separada) ou em uma VPC diferente, no seu ambiente on-premises ou pela Internet.
- Um gateway NAT comporta 5 Gbps de largura de banda e escala automaticamente até 100 Gbps. Se você precisar de mais largura de banda, poderá dividir seus recursos em várias sub-redes e criar um gateway NAT em cada sub-rede.
- Um gateway NAT pode processar um milhão de pacotes por segundo e aumentar a capacidade automaticamente para até dez milhões de pacotes por segundo. Além desse limite, um gateway NAT começará a descartar pacotes. Para evitar a perda de pacotes, divida seus recursos em várias sub-redes e crie um gateway NAT separado para cada sub-rede.
- Cada endereço IPv4 comporta até 55.000 conexões simultâneas para cada destino exclusivo. Um destino exclusivo é identificado por uma combinação exclusiva de endereço IP de destino, a porta de destino e o protocolo (TCP/UDP/ICMP). Você pode aumentar esse limite associando até 8 endereços IPv4 aos seus gateways NAT (1 endereço IPv4 primário e 7 endereços IPv4 secundários). Por padrão, há um limite de associação de 2 endereços IP elásticos ao seu gateway NAT público. É possível aumentar esse limite solicitando um ajuste de cota. Para ter mais informações, consulte Endereços IP elásticos.
- Você pode escolher o endereço IPv4 privado para atribuir ao gateway NAT ou atribuí-lo automaticamente com base no intervalo de endereços IPv4 da sub-rede. O endereço IPv4 privado atribuído persiste até que você exclua o gateway NAT privado. Não é possível desvincular o endereço IPv4 privado nem anexar endereços IPv4 privados adicionais.
- Não é possível associar um grupo de segurança a um gateway NAT. Você pode associar grupos de segurança às suas instâncias para controlar o tráfego de entrada e saída.
- Você também pode usar uma ACL de rede para controlar o tráfego que entra e sai da sub-rede para seu gateway NAT. Os gateways NAT usam as portas 1024 a 65535. Para ter mais informações, consulte Controlar o tráfego da sub-rede com listas de controle de acesso à rede.
- Um gateway NAT recebe uma interface de rede. Você pode escolher o endereço IPv4 privado para atribuir à interface ou atribuí-lo automaticamente com base no intervalo de endereços IPv4 da sub-rede. É possível visualizar a interface de rede do gateway NAT no console do Amazon EC2. Para obter mais informações, consulte Visualizar detalhes sobre uma interface de rede. Não é possível modificar os atributos da interface de rede.
- Não é possível rotear o tráfego para um gateway NAT por meio de uma conexão de emparelhamento da VPC. Não é possível rotear o tráfego por meio de um gateway NAT quando

o tráfego chega por meio de uma conexão híbrida (VPN site a site ou Direct Connect) via gateway privado virtual. É possível rotear o tráfego por meio de um gateway NAT quando o tráfego chega por meio de uma conexão híbrida (VPN site a site ou Direct Connect) via gateway de trânsito.

- Os gateways NAT oferecem suporte a tráfego com uma unidade de transmissão máxima (MTU) de 8500, mas é importante observar o seguinte:
  - A MTU de uma conexão de rede é o tamanho, em bytes, do maior pacote permissível que pode ser passado pela conexão. Quanto maior a MTU de uma conexão, mais dados podem ser passados em um único pacote.
  - Pacotes com mais de 8.500 bytes que chegam ao gateway NAT são descartados (ou fragmentados, se aplicável).
  - Para evitar possíveis perdas de pacotes ao se comunicar com recursos pela Internet usando um gateway NAT público, a configuração de MTU para suas instâncias do EC2 não deve exceder 1500 bytes. Para obter mais informações sobre como verificar e definir a MTU em uma instância, consulte Verificar e definir a MTU na instância do Linux no Guia do usuário do Amazon EC2.
  - Os gateways NAT oferecem suporte ao Path MTU Discovery (PMTUD) por meio de pacotes FRAG_NEEDED ICMPv4 e pacotes Packet Too Big (PTB) ICMPv6.
  - O gateway NAT impõe o limite de Maximum Segment Size (MSS) para todos os pacotes. Para obter mais informações, consulte RFC879.

Trabalhar com gateways NAT

Você pode usar o console da Amazon VPC para criar e gerenciar os gateways NAT.

Tarefas

- Controlar o uso de gateways NAT
- Criar um gateway NAT
- Editar associações de endereço IP secundário
- Marcar um gateway NAT
- Excluir um gateway NAT
- Visão geral da linha de comando

Controlar o uso de gateways NAT

Por padrão, os usuários do não têm permissão para trabalhar com gateways NAT. É possível criar uma política de perfil do IAM com uma política anexada que conceda permissão aos usuários para

criar, descrever e excluir gateways NAT. Para ter mais informações, consulte Identity and Access Management para o Amazon VPC.

Criar um gateway NAT

Use o procedimento a seguir para criar um gateway NAT.

Cotas relacionadas

- Você não poderá criar um gateway NAT público se tiver esgotado o número de EIPs alocados para sua conta. Para obter mais informações cotas de EIP e como ajustá-las, consulte Endereços IP elásticos.
- Você pode atribuir até 8 endereços IPv4 privados ao seu gateway NAT privado. Este limite não é ajustável.
- Por padrão, há um limite de associação de 2 endereços IP elásticos ao seu gateway NAT público. É possível aumentar esse limite solicitando um ajuste de cota. Para ter mais informações, consulte Endereços IP elásticos.

Para criar um gateway NAT

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Gateways NAT.
3. Escolha Criar um gateway NAT.
4. (Opcional) Especifique um nome para o gateway NAT. Isso cria uma tag em que a chave está **`Name`** e o valor é o nome que você especificar.
5. Selecione a sub-rede na qual o gateway NAT deve ser criado.
6. Em Tipo de conectividade, deixe a seleção padrão de Público para criar um gateway NAT público ou escolha Privado para criar um gateway NAT privado. Para obter mais informações sobre a diferença entre um gateway NAT público e um privado, consulte Gateways NAT.
7. Se você escolheu Público, faça o seguinte; caso contrário, vá para a etapa 8:

    1. Escolha um ID de alocação de IP elástico para atribuir um IP elástico ao gateway NAT ou escolha Alocar IP elástico para alocar automaticamente um IP elástico para usar em seu gateway NAT público. Por padrão, há um limite de associação de 2 endereços IP elásticos ao seu gateway NAT público. É possível aumentar esse limite solicitando um ajuste de cota. Para ter mais informações, consulte Endereços IP elásticos.

> **Important**
>
> Quando você atribui um EIP a um gateway NAT público, o grupo de borda de rede do EIP deve corresponder ao grupo de borda de rede da Zona de Disponibilidade (AZ) na qual você está iniciando o gateway NAT público. Se não for o mesmo, o gateway NAT falhará ao iniciar. Você pode ver o grupo de bordas da rede para a AZ da sub-rede visualizando os detalhes da sub-rede. Da mesma forma, você pode visualizar o grupo de bordas de rede de um EIP visualizando os detalhes do endereço EIP. Para obter mais informações sobre grupos de bordas de rede e EIPs, consulte 1. Alocar um endereço IP elástico.

2. (Opcional) Escolha Configurações adicionais e, em Endereço IP privado - opcional, insira um endereço IPv4 privado para o gateway NAT. Se você não inserir um endereço, o AWS atribuirá automaticamente um endereço IPv4 privado ao seu gateway NAT de maneira aleatória com base na sub-rede em que seu gateway NAT está.
3. Vá para a etapa 11.

8. Se você escolheu Privado, em Configurações adicionais, Método de atribuição de endereço IPv4 privado, escolha uma das seguintes opções:

   - Atribuição automática: a AWS escolhe o endereço IPv4 privado primário para o gateway NAT. Em Número de endereços IPv4 privados atribuídos automaticamente, é possível, opcionalmente, especificar o número de endereços IPv4 privados secundários para o gateway NAT. A AWS escolhe esses endereços IP aleatoriamente da sub-rede para seu gateway NAT.
   - Personalizado: em Endereço IPv4 privado principal, escolha o endereço IPv4 privado principal para o gateway NAT). Em Endereços IPv4 privados secundários, é possível, opcionalmente, especificar até 7 endereços IPv4 privados secundários para o gateway NAT.

9. Se tiver escolhido Personalizado na etapa 8, pule esta etapa. Se você escolher Atribuir automaticamente, em Número de endereços IP privados atribuídos automaticamente, escolha o número de endereços IPv4 secundários que você deseja que a AWS atribua a esse gateway NAT privado. Você pode escolher até 7 endereços IPv4.

> **Note**
>
> Os endereços IPv4 secundários são opcionais e devem ser atribuídos ou alocados quando suas workloads que usam um gateway NAT excederem 55.000 conexões simultâneas para um único destino (o mesmo IP de destino, porta de destino e

protocolo). Os endereços IPv4 secundários aumentam o número de portas disponíveis e, portanto, aumentam o limite do número de conexões simultâneas que suas workloads podem estabelecer usando um gateway NAT.

10. Se tiver escolhido Atribuir automaticamente na etapa 9, pule esta etapa. Se você escolheu Personalizado, faça o seguinte:
    1. Em Endereço IPv4 privado primário, insira o endereço IPv4 privado.
    2. Em Endereço IPv4 privado secundário, insira até 7 endereços IPv4 privados secundários.
11. (Opcional) Para adicionar uma tag ao gateway NAT, escolha Add new tag (Adicionar nova tag) e insira o nome e o valor da chave. É possível adicionar até 50 tags.
12. Escolha Criar um gateway NAT.
13. O status inicial do gateway NAT é `Pending`. Depois que o status for alterado para `Available`, o gateway NAT estará pronto para você usar. Certifique-se de atualizar as tabelas de rotas conforme necessário. Para obter exemplos, consulte the section called “Casos de uso”.

Se o status do gateway NAT mudar para `Failed`, isso significa que ocorreu um erro durante a criação. Para ter mais informações, consulte Falha na criação do gateway NAT.

Editar associações de endereço IP secundário

Cada endereço IPv4 comporta até 55.000 conexões simultâneas para cada destino exclusivo. Um destino exclusivo é identificado por uma combinação exclusiva de endereço IP de destino, a porta de destino e o protocolo (TCP/UDP/ICMP). Você pode aumentar esse limite associando até 8 endereços IPv4 aos seus gateways NAT (1 endereço IPv4 primário e 7 endereços IPv4 secundários). Por padrão, há um limite de associação de 2 endereços IP elásticos ao seu gateway NAT público. É possível aumentar esse limite solicitando um ajuste de cota. Para ter mais informações, consulte Endereços IP elásticos.

Você pode usar as métricas ErrorPortAllocation e PacketsDropCount do gateway NAT do CloudWatch para determinar se seu gateway NAT está gerando erros de alocação de portas ou descartando pacotes. Para resolver esse problema, adicione endereços IPv4 secundários ao seu gateway NAT.

Considerações

- Você pode adicionar endereços IPv4 privados secundários ao criar um gateway NAT privado ou após criar o gateway NAT usando o procedimento nesta seção. Só é possível adicionar

endereços IP elásticos secundários aos gateways NAT públicos após criar o gateway NAT usando o procedimento nesta seção.

- Seu gateway NAT pode ter até 8 endereços IPv4 associados a ele (1 endereço IPv4 primário e 7 endereços IPv4 secundários). Você pode atribuir até 8 endereços IPv4 privados ao seu gateway NAT privado. Por padrão, há um limite de associação de 2 endereços IP elásticos ao seu gateway NAT público. É possível aumentar esse limite solicitando um ajuste de cota. Para ter mais informações, consulte Endereços IP elásticos.

Para editar associações de endereços IPv4 secundários

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Gateways NAT.
3. Selecione o gateway NAT cujas associações de endereço IPv4 secundárias você deseja editar.
4. Escolha Ações e então escolha Editar associações de endereços IP secundários.
5. Se você estiver editando as associações de endereços IPv4 secundários de um gateway NAT privado, em Ação, escolha Atribuir novos endereços IPv4 ou Cancelar a atribuição de endereços IPv4 existentes. Se você estiver editando as associações de endereços IPv4 secundários de um gateway NAT público, em Ação, escolha Associar novos endereços IPv4 ou Desassociar endereços IPv4 existentes.
6. Execute um destes procedimentos:

   - Se tiver optado por atribuir ou associar novos endereços IPv4, faça o seguinte:
     1. Essa etapa é necessária. Você deve selecionar um endereço IPv4. Escolha o método de atribuição de endereço IPv4 privado:
        - Atribuir automaticamente: a AWS escolhe automaticamente um endereço IPv4 privado primário e você escolhe se deseja que a AWS atribua até 7 endereços IPv4 privados secundários para atribuir ao gateway NAT. A AWS os escolhe e atribui automaticamente para você de maneira aleatória e com base na sub-rede em que seu gateway NAT está.
        - Personalizado: escolha o endereço IPv4 privado primário e até 7 endereços IPv4 privados secundários para atribuir ao gateway NAT.
     2. Em ID de alocação de IP elástico, escolha um IP elástico para adicionar como endereço IPv4 secundário. Essa etapa é necessária. Você deve selecionar um IP elástico junto com um endereço IPv4 privado. Se você escolher Personalizado para o Método de atribuição de endereço IP privado, também deverá inserir um endereço IPv4 privado para cada IP elástico adicionado.

> **Important**
>
> Quando você atribui um EIP secundário a um gateway NAT público, o grupo de borda de rede do EIP deve corresponder ao grupo de borda de rede da Zona de Disponibilidade (AZ) na qual o gateway NAT público está. Se não for a mesma, o EIP não será atribuído. Você pode ver o grupo de bordas da rede para a AZ da sub-rede visualizando os detalhes da sub-rede. Da mesma forma, você pode visualizar o grupo de bordas de rede de um EIP visualizando os detalhes do endereço EIP. Para obter mais informações sobre grupos de bordas de rede e EIPs, consulte 1. Alocar um endereço IP elástico.

Seu gateway NAT pode ter até 8 endereços IP associados a ele. Se for um gateway NAT público, há um limite de cota padrão para IPs elásticos por região. Para ter mais informações, consulte Endereços IP elásticos.

- Se você optar por cancelar a atribuição ou desassociar novos endereços IPv4, faça o seguinte:
  1. Em Endereço IP secundário existente para cancelar a atribuição, selecione os endereços IP secundários cuja atribuição deseja cancelar.
  2. (opcional) Em Duração da drenagem de conexão, insira o tempo máximo de espera (em segundos) antes de liberar forçadamente os endereços IP se as conexões ainda estiverem em andamento. Se você não inserir um valor, o valor padrão será de 350 segundos.

7. Escolha Salvar alterações.

Se o status do gateway NAT mudar para `Failed`, isso significa que ocorreu um erro durante a criação. Para obter mais informações, consulte Falha na criação do gateway NAT.

Marcar um gateway NAT

Você pode marcar o gateway NAT para ajudar a identificá-lo ou categorizá-lo de acordo com as necessidades da organização. Para obter informações sobre como trabalhar com tags, consulte Marcar com tag os recursos do Amazon EC2 no Guia do usuário do Amazon EC2.

Há suporte a tags de alocação de custo para gateways NAT. Portanto, você também pode usar tags para organizar sua fatura da AWS e refletir sua própria estrutura de custo. Para obter mais informações, consulte Uso de tags de alocação de custos no Guia do usuário do AWS Billing. Para

obter mais informações sobre como configurar um relatório de alocação de custos com tags, consulte Relatório mensal de alocação de custos em Sobre o faturamento de contas da AWS.

Para marcar um gateway NAT

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha NAT Gateways.
3. Selecione o gateway NAT que você deseja marcar e escolha Ações. Selecione Gerenciar tags.
4. Para cada tag, escolha Adicionar nova tag e insira uma Chave e Valor para a tag. É possível adicionar até 50 tags.
5. Escolha Salvar.

Excluir um gateway NAT

Caso não precise mais de um gateway NAT, você pode excluí-lo. Depois de excluir um gateway NAT, sua entrada permanece visível no console da Amazon VPC durante um breve período (normalmente, uma hora) após o qual ela é automaticamente removida. Você não consegue removê-la.

A exclusão de um gateway NAT dissocia o respectivo endereço IP elástico, mas não libera o endereço de sua conta. Se excluir um gateway NAT, as rotas desse gateway permanecerão com o status `blackhole` até o momento em que excluir ou atualizar as rotas.

Para excluir um gateway NAT

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha NAT Gateways.
3. Selecione o botão de opção para o gateway NAT e, em seguida, escolhaActions (Ações),Delete NAT gateway (Excluir gateway NAT).
4. Quando a confirmação for solicitada, insira **`delete`** e escolha Delete (Excluir).
5. Se não for mais necessário o endereço IP elástico associado ao gateway NAT público, recomendamos que você o libere. Para ter mais informações, consulte 5. Liberar um endereço IP elástico.

Visão geral da linha de comando

É possível executar as tarefas descritas nesta página por meio da linha de comando.

Atribuir um endereço IPv4 privado a um gateway NAT

- assign-private-nat-gateway-address (AWS CLI)
- Register-EC2PrivateNatGatewayAddress (AWS Tools for Windows PowerShell)

Associar endereços IP elásticos (EIPs) e endereços IPv4 privados a um gateway NAT público

- associate-nat-gateway-address (AWS CLI)
- Register-EC2NatGatewayAddress (AWS Tools for Windows PowerShell)

Criar um gateway NAT

- create-nat-gateway (AWS CLI)
- New-EC2NatGateway (AWS Tools for Windows PowerShell)

Excluir um gateway NAT

- delete-nat-gateway (AWS CLI)
- Remove-EC2NatGateway (AWS Tools for Windows PowerShell)

Descrever um gateway NAT

- describe-nat-gateways (AWS CLI)
- Get-EC2NatGateway (AWS Tools for Windows PowerShell)

Desassociar endereços IP elásticos (EIPs) secundários de um gateway NAT público

- disassociate-nat-gateway-address (AWS CLI)
- Unregister-EC2NatGatewayAddress (AWS Tools for Windows PowerShell)

Marcar um gateway NAT

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)

Cancelar a atribuição de endereços IPv4 secundários de um gateway NAT privado

- unassign-private-nat-gateway-address (AWS CLI)
- Unregister-EC2PrivateNatGatewayAddress (AWS Tools for Windows PowerShell)

Casos de uso do gateway NAT

Os exemplos a seguir são casos de uso de gateways NAT públicos e privados.

Cenários

- Acessar a Internet a partir de uma sub-rede privada
- Acessar sua rede de endereços IP permitidos
- Habilitar a comunicação entre redes sobrepostas

Acessar a Internet a partir de uma sub-rede privada

Você pode usar um gateway NAT público para permitir que instâncias em uma sub-rede privada enviem tráfego para a Internet, enquanto impede que a Internet estabeleça conexões com essas instâncias.

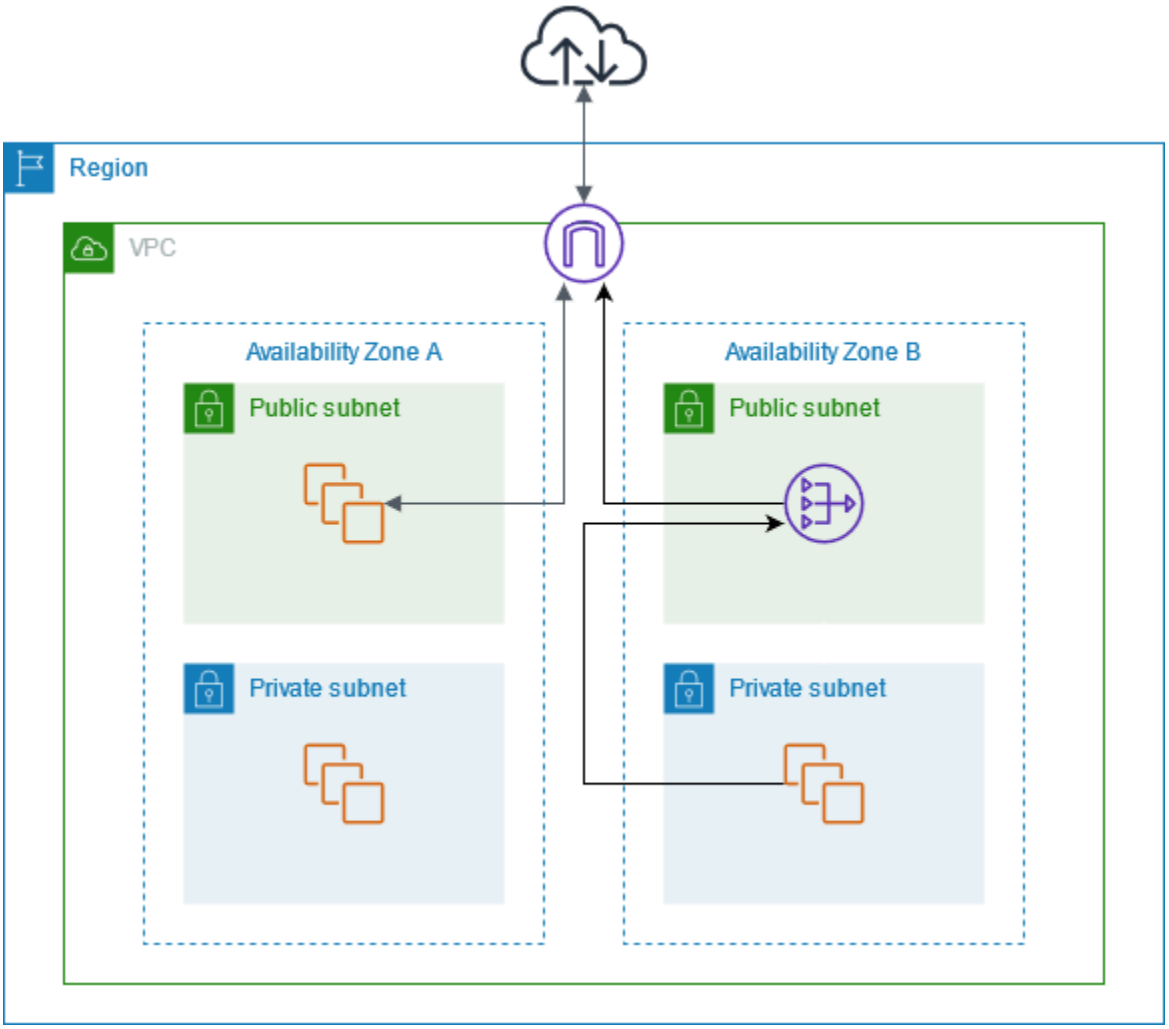
Conteúdo

- Visão geral
- Roteamento
- Testar o gateway NAT público

Visão geral

O diagrama a seguir ilustra esse caso de uso. Existem duas zonas de disponibilidade, com duas sub-redes em cada uma. A tabela de rotas para cada sub-rede determina como o tráfego é encaminhado. Na zona de disponibilidade A, as instâncias na sub-rede pública podem acessar a Internet por meio de uma rota para o gateway da Internet, enquanto as instâncias na sub-rede privada não têm rota para a Internet. Na zona de disponibilidade B, a sub-rede pública contém um gateway NAT e as instâncias na sub-rede privada podem acessar a Internet por meio de uma rota para o gateway NAT na sub-rede pública. Os gateways NAT privados e públicos mapeiam o endereço IPv4 privado de origem das instâncias para o endereço IPv4 privado do gateway NAT privado, mas no caso de um gateway NAT público, o gateway da Internet mapeia o endereço IPv4 privado do gateway NAT

público para o endereço IP elástico associado ao gateway NAT. Ao enviar tráfego de resposta para as instâncias, seja um gateway NAT público ou privado, o gateway NAT converte o endereço de volta para o endereço IP de origem inicial.



Observe que, se as instâncias na sub-rede privada na zona de disponibilidade A também precisarem acessar a Internet, você poderá criar uma rota dessa sub-rede para o gateway NAT na zona de disponibilidade B. Como alternativa, é possível melhorar a resiliência criando um gateway NAT em cada zona de disponibilidade que contenha recursos que exigem acesso à Internet. Para ver um exemplo de diagrama, consulte the section called “Servidores privados”.

Roteamento

A tabela de rotas a seguir está associada à sub-rede pública na zona de disponibilidade A. A primeira entrada é a rota local. Ela permite que as instâncias na sub-rede se comuniquem com outras instâncias na VPC usando endereços IP privados. A segunda entrada envia todo o outro tráfego

da sub-rede para o gateway da Internet; o que permite que as instâncias na sub-rede acessem a Internet.

Destino	Alvo
CIDR DA VPC	local
0.0.0.0/0	*internet-gateway-id*

A tabela de rotas a seguir está associada à sub-rede privada na zona de disponibilidade A. A entrada é a rota local, que permite que as instâncias na sub-rede se comuniquem com outras instâncias na VPC usando endereços IP privados. As instâncias nessa sub-rede não têm acesso à Internet.

Destino	Alvo
CIDR DA VPC	local

A tabela de rotas a seguir está associada à sub-rede pública na zona de disponibilidade B. A primeira entrada é a rota local. Ela permite que as instâncias na sub-rede se comuniquem com outras instâncias na VPC usando endereços IP privados. A segunda entrada envia todo o outro tráfego da sub-rede para o gateway da Internet; o que permite que o gateway NAT na sub-rede acesse a Internet.

Destino	Alvo
CIDR DA VPC	local
0.0.0.0/0	*internet-gateway-id*

A tabela de rotas a seguir está associada à sub-rede privada na zona de disponibilidade B. A primeira entrada é a rota local. Ela permite que as instâncias na sub-rede se comuniquem com outras instâncias na VPC usando endereços IP privados. A segunda entrada envia todos os outros tráfegos da sub-rede ao gateway NAT.

Destino	Alvo
CIDR DA VPC	local
0.0.0.0/0	*nat-gateway-id*

Para ter mais informações, consulte the section called “Alterar a tabela de rotas de uma sub-rede”.

Testar o gateway NAT público

Após criar o gateway NAT e atualizar as tabelas de rotas, você poderá executar ping endereços remotos na internet de uma instância na sua sub-rede privada para testar se ela pode se conectar à Internet. Para obter um exemplo de como fazer isso, consulte Testar a conexão com a internet.

Se conseguir conectar à Internet, você também poderá testar se o tráfego da Internet é roteado via gateway NAT:

- rastreie a rota do tráfego de uma instância em sua sub-rede privada. Para isso, execute o comando `traceroute` em uma instância Linux em sua sub-rede privada. Na saída, você deve ver o endereço IP privado do gateway NAT em um dos saltos (em geral, o primeiro salto).
- Use um site ou uma ferramenta de terceiros que exiba o endereço IP de origem quando você se conecta a ele de uma instância de sua sub-rede privada. O endereço IP de origem deve ser o endereço IP elástico do seu gateway NAT.

Se esses testes falharem, consulte Solucionar problemas de gateways NAT.

Testar a conexão com a internet

O exemplo a seguir demonstra como testar se uma instância em uma sub-rede privada pode se conectar com a Internet.

1. Execute uma instância em sua sub-rede pública (use-a como bastion host). No Launch Wizard, é necessário selecionar uma AMI do Amazon Linux e atribuir um endereço IP público à instância. Verifique se as regras do grupo de segurança permitem tráfego SSH de entrada do intervalo de endereços IP de sua rede local e tráfego SSH de saída para o intervalo de endereços IP da sub-rede privada (você também pode usar `0.0.0.0/0` para tráfego SSH de entrada e de saída para este teste).

2. Execute uma instância em sua sub-rede privada. No Launch Wizard, selecione uma Amazon Linux AMI. Não atribua um endereço IP público à sua instância. Confirme se as regras de seu grupo de segurança permitem tráfego SSH de entrada do intervalo de endereços IP privados da instância que você executou na sub-rede pública e todos os tráfegos ICMP de saída. Você deve escolher o mesmo par de chaves que usou para executar sua instância na sub-rede pública.
3. Configure o encaminhamento de agente SSH no computador local e conecte-se ao bastion host na sub-rede pública. Para obter mais informações, consulte Para configurar o encaminhamento de agente SSH para Linux ou macOS ou Configurar o encaminhamento de agente SSH para Windows.
4. No bastion host, conecte-se à instância na sub-rede privada e teste a conexão com a internet na instância na sub-rede privada. Para obter mais informações, consulte Para testar a conexão com a internet.

Para configurar o encaminhamento de agente SSH para Linux ou macOS

1. Em seu computador local, adicione sua chave privada para o agente de autenticação.

   No Linux, use o comando a seguir:

   ```
   ssh-add -c mykeypair.pem
   ```

   No macOS, use o comando a seguir:

   ```
   ssh-add -K mykeypair.pem
   ```

2. Conecte-se à sua instância na sub-rede pública usando a opção `-A` para permitir o encaminhamento de agente SSH e use o endereço público da instância, conforme mostrado no exemplo a seguir.

   ```
   ssh -A ec2-user@54.0.0.123
   ```

Configurar o encaminhamento de agente SSH para Windows

Você pode usar o cliente OpenSSH disponível no Windows ou instalar seu cliente SSH preferencial (por exemplo, PuTTY).

OpenSSH

Instale o OpenSSH para Windows conforme descrito neste artigo: Getting started with OpenSSH for Windows. Em seguida, adicione sua chave ao agente de autenticação. Para obter mais informações, consulte Key-based authentication in OpenSSH for Windows.

PuTTY

1. Faça download e instale o Pageant na página de download PuTTY, se ele ainda não estiver instalado.
2. Converta sua chave privada no formato .ppk. Para obter mais informações, consulte Converter a chave privada usando o PuTTYgen no Guia do usuário do Amazon EC2.
3. Inicie o Pageant, clique com o botão direito no ícone do Pageant na barra de tarefas (ele pode estar oculto) e escolha Add Key. Selecione o arquivo .ppk que você criou, digite a senha se necessário e escolha Open (Abrir).
4. Inicie a sessão PuTTY session e conecte-se à sua instância na sub-rede pública usando o respectivo endereço IP. Para obter mais informações, consulte Conectar-se à instância do Linux usando PuTTY. Na categoria Auth, selecione a opção Allow agent forwarding e deixe a caixa Private key file for authentication em branco.

Para testar a conexão com a internet

1. Em sua instância na sub-rede pública, conecte-se à sua instância na sub-rede privada usando o endereço IP privado, conforme mostrado no exemplo a seguir.

```
ssh ec2-user@10.0.1.123
```

2. Na instância privada, teste se é possível conectar-se à Internet executando o comando `ping` para um site que tenha o ICMP habilitado.

```
ping ietf.org
```

```
PING ietf.org (4.31.198.44) 56(84) bytes of data.
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=1 ttl=47 time=86.0 ms
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=2 ttl=47 time=75.6 ms
...
```

Pressione Ctrl+C no teclado para cancelar o comando `ping`. Se o comando `ping` falhar, consulte As instâncias não conseguem acessar a Internet.

3. (Opcional) Se você não precisar mais das instâncias, termine-as. Para obter mais informações, consulte Terminar sua instância no Guia do usuário do Amazon EC2.

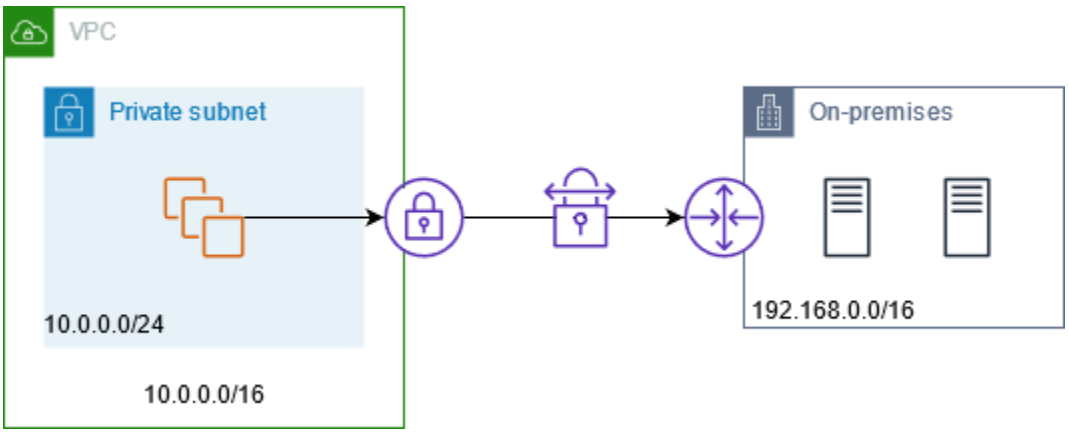
Acessar sua rede de endereços IP permitidos

Você pode usar um gateway NAT privado para permitir a comunicação de suas VPCs para sua rede on-premises usando um grupo de endereços permitidos. Em vez de atribuir a cada instância um endereço IP separado do intervalo de endereços IP permitidos, você pode rotear o tráfego da sub-rede destinado à rede on-premises por meio de um gateway NAT privado, com um endereço IP do intervalo de endereços IP permitidos.

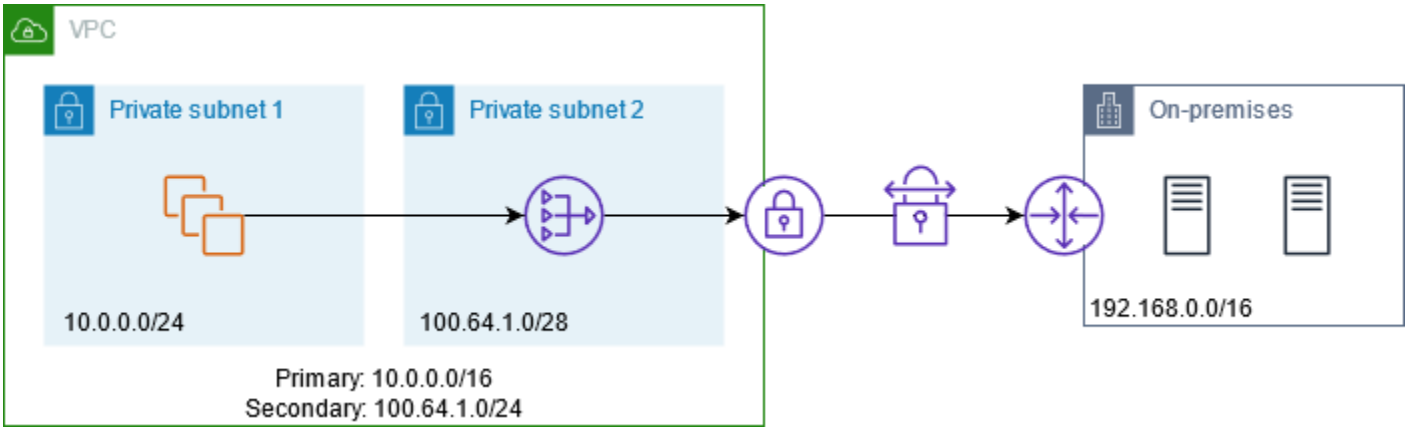
Conteúdo

Visão geral

O diagrama a seguir mostra como as instâncias podem acessar os recursos on-premises por meio da AWS VPN. O tráfego das instâncias é roteado para um gateway privado virtual, pela conexão VPN, para o gateway do cliente e, em seguida, para o destino na rede on-premises. No entanto, suponha que o destino permita tráfego somente de um intervalo de endereços IP específico, como 100.64.1.0/28. Isso impediria que o tráfego dessas instâncias chegasse à rede on-premises.



O diagrama a seguir mostra os principais componentes da configuração deste cenário. A VPC tem seu intervalo de endereços IP original e o intervalo de endereços IP permitidos. A VPC tem uma sub-rede do intervalo de endereços IP permitidos com um gateway NAT privado. O tráfego das instâncias destinadas à rede on-premises é enviado para o gateway NAT antes de ser roteado para a conexão VPN. A rede on-premises recebe o tráfego das instâncias com o endereço IP de origem do gateway NAT, que está no intervalo de endereços IP permitidos.



Recursos

Crie ou atualize recursos da seguinte maneira:

- Associe o intervalo de endereços IP permitidos à VPC.
- Crie uma sub-rede na VPC do intervalo de endereços IP permitidos.
- Crie um gateway NAT privado na nova sub-rede.
- Atualize a tabela de rotas para a sub-rede com as instâncias, para enviar tráfego destinado à rede on-premises para o gateway NAT. Adicione uma rota à tabela de rotas para a sub-rede com o gateway NAT privado que envia o tráfego destinado à rede on-premises para o gateway privado virtual.

Roteamento

A tabela de rotas a seguir está associada à primeira sub-rede. Existe uma rota local para cada CIDR da VPC. As rotas locais permitem que os recursos na sub-rede se comuniquem com outros recursos na VPC usando endereços IP privados. A terceira entrada envia tráfego destinado à rede on-premises para o gateway NAT privado.

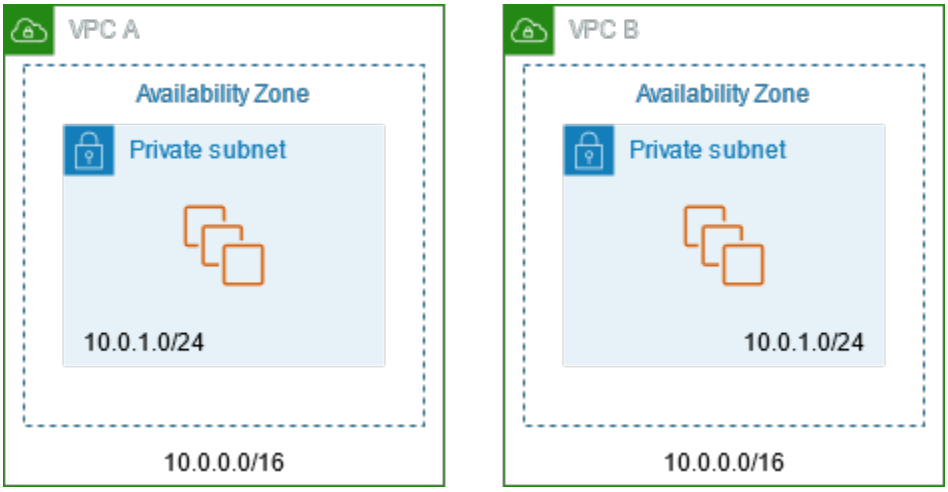
Destino	Destino
10.0.0.0/16	local
100.64.1.0/24	local
192.168.0.0/16	*nat-gateway-id*

A tabela de rotas a seguir está associada à segunda sub-rede. Existe uma rota local para cada CIDR da VPC. As rotas locais permitem que os recursos na sub-rede se comuniquem com outros recursos na VPC usando endereços IP privados. A terceira entrada envia o tráfego destinado à rede on-premises para o gateway privado virtual.

Destino	Destino
10.0.0.0/16	local
100.64.1.0/24	local
192.168.0.0/16	*vgw-id*

Habilitar a comunicação entre redes sobrepostas

Você pode usar um gateway NAT privado para habilitar a comunicação entre redes, mesmo se elas tiverem intervalos CIDR sobrepostos. Por exemplo, suponha que as instâncias na VPC A precisem acessar os serviços fornecidos pelas instâncias na VPC B.



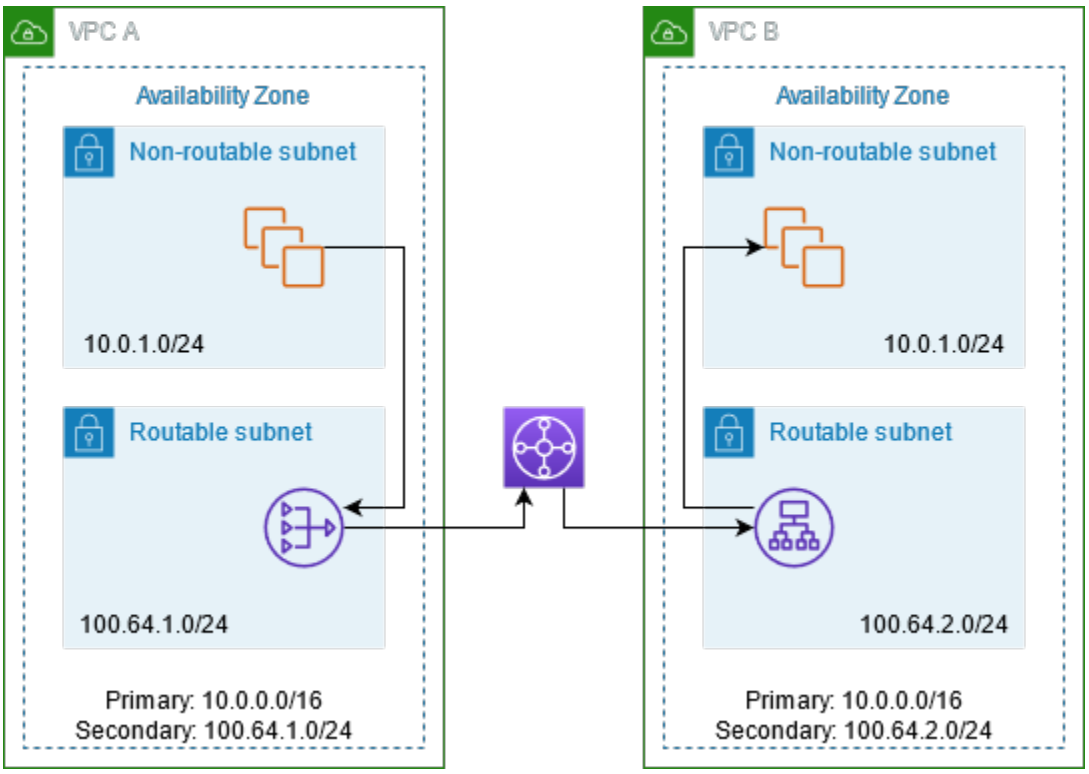
Conteúdo

Visão geral

O diagrama a seguir mostra os principais componentes da configuração deste cenário. Primeiro, sua equipe de gerenciamento de IP determina quais intervalos de endereços podem se sobrepor (intervalos de endereços não roteáveis) e quais não podem (intervalos de endereços roteáveis). A equipe de gerenciamento de IP aloca intervalos de endereços do grupo de intervalos de endereços roteáveis a projetos, mediante solicitação.

Cada VPC tem seu intervalo de endereços IP original, que não é roteável, além do intervalo de endereços IP roteáveis atribuído a ela pela equipe de gerenciamento de IP. A VPC A tem uma sub-rede de seu intervalo roteável com um gateway NAT privado. O gateway NAT privado obtém seu endereço IP de sua sub-rede. A VPC B tem uma sub-rede de seu intervalo roteável com um Application Load Balancer. O Application Load Balancer obtém seus endereços IP de suas sub-redes.

O tráfego de uma instância na sub-rede não roteável da VPC A destinada às instâncias na sub-rede não roteável da VPC B é enviado por meio do gateway NAT privado e, em seguida, roteado para o gateway de trânsito. O gateway de trânsito envia o tráfego ao Application Load Balancer, que o roteia a uma das instâncias de destino na sub-rede não roteável da VPC B. O tráfego do gateway de trânsito para o Application Load Balancer tem o endereço IP de origem do gateway NAT privado. Portanto, o tráfego de resposta do balanceador de carga usa o endereço do gateway NAT privado como destino. O tráfego de resposta é enviado para o gateway de trânsito e, em seguida, roteado para o gateway NAT privado, que traduz o destino para a instância na sub-rede não roteável da VPC A.



Recursos

Crie ou atualize recursos da seguinte maneira:

- Associe os intervalos de endereços IP roteáveis atribuídos às respectivas VPCs.
- Crie uma sub-rede na VPC A de seu intervalo de endereços IP roteáveis e crie um gateway NAT privado nessa nova sub-rede.
- Crie uma sub-rede na VPC B de seu intervalo de endereços IP roteáveis e crie um Application Load Balancer nessa nova sub-rede. Registre as instâncias na sub-rede não roteável com o grupo de destino para o balanceador de carga.
- Crie um gateway de trânsito para conectar as VPCs. Certifique-se de desabilitar a propagação de rotas. Quando você anexar cada VPC ao gateway de trânsito, use o intervalo de endereços roteáveis da VPC.
- Atualize a tabela de rotas da sub-rede não roteável na VPC A para enviar todo o tráfego destinado ao intervalo de endereços roteáveis da VPC B para o gateway NAT privado. Atualize a tabela de rotas da sub-rede roteável na VPC A para enviar todo o tráfego destinado ao intervalo de endereços roteáveis da VPC B para o gateway de trânsito.
- Atualize a tabela de rotas da sub-rede roteável na VPC B para enviar todo o tráfego destinado ao intervalo de endereços roteáveis da VPC A para o gateway de trânsito.

Roteamento

A tabela a seguir é a tabela de rotas para a sub-rede não roteável na VPC A.

Destino	Destino
10.0.0.0/16	local
100.64.1.0/24	local
100.64.2.0/24	*nat-gateway-id*

A tabela a seguir é a tabela de rotas para a sub-rede roteável na VPC A.

Destino	Destino
10.0.0.0/16	local
100.64.1.0/24	local
100.64.2.0/24	*transit-gateway-id*

A tabela a seguir é a tabela de rotas para a sub-rede não roteável na VPC B.

Destino	Destino
10.0.0.0/16	local
100.64.2.0/24	local

A tabela a seguir é a tabela de rotas para a sub-rede roteável na VPC B.

Destino	Destino
10.0.0.0/16	local
100.64.2.0/24	local

Destino	Destino
100.64.1.0/24	*transit-gateway-id*

Veja a seguir a tabela de rotas de gateway de trânsito.

CIDR	Attachment	Tipo de rota
100.64.1.0/24	*Anexo para a VPC A*	Estático
100.64.2.0/24	*Anexo para a VPC B*	Estático

DNS64 e NAT64

Um gateway NAT oferece suporte à conversão de endereços de rede de IPv6 para IPv4, mais conhecida como NAT64. A NAT64 ajuda os seus recursos IPv6 da AWS a se comunicarem com recursos IPv4 na mesma VPC ou em uma VPC diferente, na sua rede on-premises ou pela Internet. Você pode usar a NAT64 com o DNS64 no Amazon Route 53 Resolver ou o seu próprio servidor DNS64.

Conteúdo

O que é o DNS64?

As suas workloads somente IPv6 em execução em VPCs só podem enviar e receber pacotes de rede IPv6. Sem o DNS64, uma consulta de DNS para um serviço somente IPv4 produzirá um endereço de destino IPv4 em resposta e seu serviço somente IPv6 não poderá se comunicar com ele. Para preencher essa lacuna de comunicação, você pode habilitar o DNS64 para uma sub-rede e ela se aplica a todos os recursos da AWS dentro dessa sub-rede. Com o DNS64, o Amazon Route 53 Resolver procura o registro DNS do serviço que você consultou e segue um dos seguintes procedimentos:

- Se o registro contiver um endereço IPv6, ele retornará o registro original e a conexão será estabelecida sem nenhuma conversão por IPv6.
- Se não houver um endereço IPv6 associado ao destino no registro DNS, o Route 53 Resolver sintetizará um endereço acrescentando o prefixo conhecido `/96`, definido em RFC6052 (`64:ff9b::/96`), ao endereço IPv4 presente no registro. O seu serviço somente IPv6 envia pacotes de rede para o endereço IPv6 sintetizado. Em seguida, você precisará encaminhar esse tráfego através do gateway NAT, que executa a conversão necessária no tráfego para permitir que os serviços IPv6 em sua sub-rede acessem serviços IPv4 fora dessa sub-rede.

É possível habilitar ou desabilitar o DNS64 em uma sub-rede usando modify-subnet-attribute com a AWS CLI ou com o console da VPC selecionando uma sub-rede e escolhendo Actions > Modify DNS64 settings (Ações > Modificar configurações de DNS64).

O que é a NAT64?

A NAT64 habilita a comunicação de seus serviços somente IPv6 em Amazon VPCs com serviços somente IPv4 dentro da mesma VPC (em sub-redes diferentes) ou VPCs conectadas, em suas redes on-premises ou pela Internet.

A NAT64 está disponível automaticamente em seus gateways NAT existentes ou em qualquer novo gateway NAT que você criar. Não é possível habilitar ou desabilitar esse recurso. A sub-rede na qual o gateway NAT está não precisa ser uma sub-rede de pilha dupla para que o NAT64 funcione.

Depois que você ativar o DNS64, se o serviço somente IPv6 enviar pacotes de rede para um endereço IPv6 sintetizado por meio do gateway NAT, ocorrerá o seguinte:

- Com o prefixo `64:ff9b::/96`, o gateway NAT reconhece que o destino original é IPv4 e converte os pacotes IPv6 em IPv4 substituindo:
  - O IPv6 de origem com seu próprio IP privado, que é convertido para o endereço IP elástico pelo gateway da Internet.
  - O IPv6 de destino para o IPv4 truncando o prefixo `64:ff9b::/96`.
- O gateway NAT envia os pacotes IPv4 convertidos para o destino por meio do gateway da Internet, gateway privado virtual ou gateway de trânsito e inicia uma conexão.
- O host somente IPv4 envia os pacotes IPv4 de resposta de volta. Depois que uma conexão é estabelecida, o gateway NAT aceita os pacotes IPv4 de resposta dos hosts externos.
- Os pacotes IPv4 de resposta são destinados ao gateway NAT, que os recebe e desfaz sua conversão substituindo seu IP (IP de destino) pelo endereço IPv6 do host e acrescentando

`64:ff9b::/96` de volta ao endereço IPv4 de origem. O pacote então vai até o host seguindo a rota local.

Dessa forma, o gateway NAT permite que suas workloads somente IPv6 em uma sub-rede se comuniquem com serviços somente IPv4 fora da sub-rede.

Configure o DNS64 e a NAT64

Siga as etapas desta seção para configurar o DNS64 e a NAT64 para habilitar a comunicação com serviços somente IPv4.

Conteúdo

- Habilitar a comunicação com serviços somente IPv4 pela Internet com a AWS CLI
- Habilite a comunicação com serviços somente IPv4 em seu ambiente on-premises

Habilitar a comunicação com serviços somente IPv4 pela Internet com a AWS CLI

Se você tiver uma sub-rede com workloads somente IPv6 que precise se comunicar com serviços somente IPv4 fora da sub-rede, este exemplo mostra como habilitar os serviços somente IPv6 para a comunicação com serviços somente IPv4 pela Internet.

Primeiro, você deve configurar um gateway NAT em uma sub-rede pública (separada da sub-rede que contém as workloads somente IPv6). Por exemplo, a sub-rede que contém o gateway NAT deve ter uma rota `0.0.0.0/0` apontando para o gateway da Internet.

Conclua estas etapas para permitir que esses serviços somente IPv6 se conectem a serviços somente IPv4 pela Internet:

1. Adicione as três rotas a seguir à tabela de rotas da sub-rede que contém as workloads somente IPv6:
   - Rota IPv4 (se houver) apontando para o gateway NAT.
   - Rota `64:ff9b::/96` apontando para o gateway NAT. Isso permitirá que o tráfego de suas workloads somente IPv6 destinadas a serviços somente IPv4 seja roteado por meio do gateway NAT.
   - Rota IPv6 `::/0` apontando para o gateway da Internet somente de saída (ou o gateway da Internet).

Observe que apontar `::/0` para o gateway da Internet permitirá que hosts IPv6 externos (fora da VPC) iniciem a conexão por IPv6.

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-cidr-block
0.0.0.0/0 --nat-gateway-id nat-05dba92075d71c408
```

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-ipv6-cidr-block
64:ff9b::/96 --nat-gateway-id nat-05dba92075d71c408
```

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-ipv6-cidr-block
::/0 --egress-only-internet-gateway-id eigw-c0a643a9
```

2. Habilite o recurso do DNS64 na sub-rede que contém as workloads somente IPv6.

```
aws ec2 modify-subnet-attribute --subnet-id subnet-1a2b3c4d --enable-dns64
```

Agora, os recursos na sua sub-rede privada podem estabelecer conexões com estado com serviços IPv4 e IPv6 pela Internet. Configure o seu grupo de segurança e NACLs adequadamente para permitir o tráfego de saída e entrada ao tráfego de `64:ff9b::/96`.

Habilite a comunicação com serviços somente IPv4 em seu ambiente on-premises

O Amazon Route 53 Resolver permite que você encaminhe consultas de DNS da sua VPC para uma rede on-premises e vice-versa. Para isso, você pode fazer o seguinte:

- Você cria um endpoint de saída do Route 53 Resolver em uma VPC e atribui a ele os endereços IPv4 dos quais deseja que o Route 53 Resolver encaminhe consultas. Para o seu resolvedor de DNS on-premises, estes são os endereços IP dos quais as consultas de DNS se originam e, portanto, devem ser endereços IPv4.
- Você cria uma ou mais regras que especifiquem os nomes de domínio das consultas de DNS que deseja que o Route 53 Resolver encaminhe aos seus resolvedores on-premises. Também é necessário especificar os endereços IPv4 dos resolvedores on-premises.

- Agora que você configurou um endpoint de saída do Route 53 Resolver, é preciso habilitar o DNS64 na sub-rede que contém suas workloads somente IPv6 e encaminhar todos os dados destinados à sua rede on-premises por meio de um gateway NAT.

Como o DNS64 funciona para destinos somente IPv4 em redes on-premises:

1. Você atribui um endereço IPv4 ao endpoint de saída do Route 53 Resolver na sua VPC.
2. A consulta de DNS do seu serviço IPv6 vai para o Route 53 Resolver por IPv6. O Route 53 Resolver corresponde à consulta com a regra de encaminhamento e obtém um endereço IPv4 para o seu resolvedor on-premises.
3. O Route 53 Resolver converte o pacote de consulta de IPv6 para IPv4 e o encaminha para o endpoint de saída. Cada endereço IP do endpoint representa um ENI que encaminha a solicitação ao endereço IPv4 on-premises do seu revolvedor de DNS.
4. O revolvedor on-premises envia o pacote de resposta por IPv4 de volta pelo endpoint de saída para o Route 53 Resolver.
5. Caso a consulta tenha sido feita por meio de uma sub-rede habilitada para DNS64, o Route 53 Resolver fará duas coisas:

    a. Ele verifica o conteúdo do pacote de resposta. Se houver um endereço IPv6 no registro, ele manterá o conteúdo como está, se ele contiver apenas um registro IPv4. Ele também sintetiza um registro IPv6 acrescentando `64:ff9b::/96` ao endereço IPv4.

    b. Ele reempacota o conteúdo e o envia para o serviço na sua VPC por IPv6.

Monitorar gateways NAT com o Amazon CloudWatch

É possível monitorar o gateway NAT usando o CloudWatch, que coleta informações do gateway NAT e cria métricas legíveis quase em tempo real. Você pode usar essas informações para monitorar e resolver problemas do gateway NAT. Essas métricas oferecem visibilidade da integridade e do desempenho do seu gateway NAT, permitindo que você monitore de perto sua operação e solucione rapidamente quaisquer problemas.

As métricas do gateway NAT coletadas pelo CloudWatch incluem pontos de dados como bytes processados, contagens de pacotes, contagens de conexões e taxas de erro. Isso permite que você entenda completamente o tráfego que flui pelo gateway NAT e identifique quaisquer anomalias ou gargalos. O CloudWatch fornece esses dados métricos em intervalos de 1 minuto, oferecendo uma visão granular e atualizada do comportamento do seu gateway NAT.

Além disso, o CloudWatch retém esses dados métricos do gateway NAT por um período prolongado de 15 meses, permitindo que você analise tendências e padrões ao longo do tempo. É possível usar esses dados históricos para planejar a capacidade, otimizar a performance e entender a evolução de longo prazo do uso do gateway NAT.

Para aproveitar esses poderosos recursos de monitoramento, você pode criar painéis e alarmes personalizados do CloudWatch adaptados às suas necessidades específicas. Por exemplo, é possível configurar alertas para notificar sempre que a transferência de dados de saída do gateway NAT exceder um determinado limite, permitindo que você resolva proativamente possíveis restrições de largura de banda.

Para obter mais informações sobre a definição de preço, consulte Preços do Amazon CloudWatch.

Conteúdo

Métricas e dimensões do gateway NAT

As métricas a seguir estão disponíveis para os gateways NAT. A coluna de descrição inclui uma descrição de cada métrica, bem como as unidades e as estatísticas.

Métrica	Descrição
`ActiveConnectionCount`	O número total de conexões TCP simultâneas e ativos por meio do gateway NAT. O valor zero indica que não há conexão ativas por meio do gateway NAT. Unidades: contagem Statistics: a estatística mais útil é `Max`.
`BytesInFromDestination`	O número de bytes recebidos pelo gateway NAT do destino.

Métrica	Descrição
	Se o valor para `BytesOutToSource` for menor que o valor de `BytesInFromDestination`, talvez haja perda de dados durante o processamento do gateway NAT ou tráfego sendo ativamente bloqueado pelo gateway NAT. Unidades: bytes Statistics: a estatística mais útil é `Sum`.
`BytesInFromSource`	O número de bytes recebidos pelo gateway NAT dos clientes na VPC. Se o valor de `BytesOutToDestination` for menor que o valor de `BytesInFromSource`, poderá haver perda de dados durante o processamento do gateway NAT. Unidades: bytes Statistics: a estatística mais útil é `Sum`.
`BytesOutToDestination`	O número de bytes enviados por meio do gateway NAT ao destino. Um valor maior que zero indica que há tráfego fluindo dos clientes que estão atrás do gateway NAT para a Internet. Se o valor de `BytesOutToDestination` for menor que o valor de `BytesInFromSource`, poderá haver perda de dados durante o processamento do gateway NAT. Unidade: bytes Statistics: a estatística mais útil é `Sum`.

Métrica	Descrição
BytesOutToSource	O número de bytes enviados por meio do gateway NAT para os clientes na VPC. Um valor maior que zero indica que há tráfego fluindo da Internet para os clientes que estão atrás do gateway NAT. Se o valor para BytesOutToSource for menor que o valor de BytesInFromDestination, talvez haja perda de dados durante o processamento do gateway NAT ou tráfego sendo ativamente bloqueado pelo gateway NAT. Unidades: bytes Statistics: a estatística mais útil é Sum.
ConnectionAttemptCount	O número de tentativas de conexão feita por meio do gateway NAT. Se o valor de ConnectionEstablishedCount for menor que o valor de ConnectionAttemptCount, os clientes atrás do gateway NAT tentaram estabelecer novas conexões para as quais não houve resposta. Unidade: contagem Statistics: a estatística mais útil é Sum.

Métrica	Descrição
ConnectionEstablishedCount	O número de conexões estabelecidas por meio do gateway NAT. Se o valor de ConnectionEstablishedCount for menor que o valor de ConnectionAttemptCount, os clientes atrás do gateway NAT tentaram estabelecer novas conexões para as quais não houve resposta. Unidade: contagem Statistics: a estatística mais útil é Sum.
ErrorPortAllocation	O número de vezes que o gateway NAT não conseguiu alocar uma porta de origem. Um valor maior de zero indica que muitas conexões simultâneas são abertas por meio do gateway NAT. Unidades: contagem Statistics: a estatística mais útil é Sum.

Métrica	Descrição
`IdleTimeoutCount`	O número de conexões que fizeram a transição do estado ativo para o estado inativo. Uma conexão ativa faz a transição para estado inativo caso não tenha sido fechada corretame nte e não haja atividade por pelo menos 350 segundos. Um valor maior que zero indica que há conexões que foram movidas para um estado inativo. Se o valor de `IdleTimeoutCount` aumentar, isso pode indicar que os clientes atrás do gateway NAT estejam reutilizando conexões obsoletas. Unidade: contagem Statistics: a estatística mais útil é `Sum`.

Métrica	Descrição
`PacketsDropCount`	O número de pacotes removidos pelo gateway NAT. Para calcular o número de pacotes descartados como uma porcentagem do tráfego geral de pacotes, use esta fórmula: `PacketsDropCount/(PacketsInFromSource+PacketsInFromDestination)*100`. Se esse valor exceder 0,01% do tráfego total no gateway NAT, é possível que haja um problema com o serviço da Amazon VPC. Use o Painel de integridade do serviço da AWS para identificar quaisquer problemas com o serviço que possam estar fazendo com que os gateways NAT descartem pacotes. Unidades: contagem Statistics: a estatística mais útil é `Sum`.
`PacketsInFromDestination`	O número de pacotes recebidos pelo gateway NAT do destino. Se o valor para `PacketsOutToSource` for menor que o valor de `PacketsInFromDestination`, talvez haja perda de dados durante o processamento do gateway NAT ou tráfego sendo ativamente bloqueado pelo gateway NAT. Unidade: contagem Statistics: a estatística mais útil é `Sum`.

Métrica	Descrição
PacketsInFromSource	O número de pacotes recebidos pelo gateway NAT dos clientes na VPC. Se o valor de PacketsOutToDestination for menor que o valor de PacketsInFromSource, poderá haver perda de dados durante o processamento do gateway NAT. Unidade: contagem Statistics: a estatística mais útil é Sum.
PacketsOutToDestination	O número de pacotes enviados por meio do gateway NAT ao destino. Um valor maior que zero indica que há tráfego fluindo dos clientes que estão atrás do gateway NAT para a Internet. Se o valor de PacketsOutToDestination for menor que o valor de PacketsInFromSource, poderá haver perda de dados durante o processamento do gateway NAT. Unidade: contagem Statistics: a estatística mais útil é Sum.

Métrica	Descrição
PacketsOutToSource	O número de pacotes enviados por meio do gateway NAT para os clientes na VPC. Um valor maior que zero indica que há tráfego fluindo da Internet para os clientes que estão atrás do gateway NAT. Se o valor para PacketsOutToSource for menor que o valor de PacketsInFromDestination, talvez haja perda de dados durante o processamento do gateway NAT ou tráfego sendo ativamente bloqueado pelo gateway NAT. Unidade: contagem Statistics: a estatística mais útil é Sum.
PeakBytesPerSecond	Essa métrica relata a maior média de bytes por segundo de 10 segundos em um determinado minuto. Unidades: contagem Statistics: a estatística mais útil é Maximum.
PeakPacketsPerSecond	Essa métrica calcula a taxa média de pacotes (pacotes processados por segundo) a cada 10 segundos por 60 segundos e depois relata o máximo das seis taxas (a maior taxa média de pacotes). Unidades: contagem Statistics: a estatística mais útil é Maximum.

Para filtrar os dados das métricas, use a dimensão a seguir.

Dimensão	Descrição
`NatGatewayId`	Filtre os dados da métrica pelo ID do gateway NAT.

Visualizar métricas do CloudWatch do gateway NAT

As métricas do gateway NAT são enviadas ao CloudWatch em intervalos de um minuto. As métricas são agrupadas primeiramente pelo namespace do serviço e, em seguida, pelas possíveis combinações de dimensões dentro de cada namespace. Você pode visualizar as métricas dos gateways NAT da maneira a seguir.

Para visualizar indicadores usando o console do CloudWatch

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Metrics (Métricas), All metrics (Todas as métricas).
3. Escolha o namespace de métrica NatGateway.
4. Escolha uma dimensão da métrica.

Para visualizar métricas usando o AWS CLI

Em um prompt de comando, use o comando a seguir para listar as métricas que estão disponíveis para o serviço do gateway NAT.

```
aws cloudwatch list-metrics --namespace "AWS/NATGateway"
```

Criar alarmes do CloudWatch para monitorar o gateway NAT

Você pode criar um alarme do CloudWatch que envia uma mensagem do Amazon SNS quando o alarme muda de estado. Um alarme observa uma única métrica por um período tempo que você especifica. Ele envia uma notificação a um tópico do Amazon SNS com base no valor da métrica em relação a um limite especificado em um número de períodos.

Por exemplo, você pode criar um alarme que monitore a quantidade de tráfego de entrada ou de saída do gateway NAT. O alarme a seguir monitora a quantidade de tráfego de saída de clientes na VPC através do gateway NAT para a internet. Ele envia uma notificação quando o número de bytes atinge um limite de 5.000.000 em um período de 15 minutos.

Para criar um alarme para o tráfego de saída através do gateway NAT

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Alarms (Alarmes), All alarms (Todos os alarmes).
3. Selecione Criar alarme.
4. Escolha Selecionar métrica.
5. Escolha o namespace de métrica NATGateway e, em seguida, escolha uma dimensão de métrica. Quando você chegar às métricas, marque a caixa de seleção ao lado da métrica BytesouttoDestination para o gateway NAT e, em seguida, escolha Select metric (Selecionar métrica).
6. Configure o alarme como indicado a seguir e, em seguida, selecione Avançar:
   - Em Estatística, selecione Soma.
   - Em Period (Período), escolha 15 minutes (15 minutos).
   - Em Whenever (Sempre que), escolha Greater/Equal (Maior que/igual a) e insira `5000000` como limite.
7. Em Notification (Notificação), escolha um tópico existente do SNS ou Create new topic (Criar tópico) para criar um. Escolha Próximo.
8. Insira um nome e uma descrição para o alarme e selecione Next (Avançar).
9. Quando você terminar de configurar o alarme, escolha Create alarm (Criar alarme).

Como outro exemplo, você pode criar um alarme que monitore erros de alocação de porta e envie uma notificação quando o valor for maior que zero (0) por três períodos de cinco minutos consecutivos.

Para criar um alarme para monitorar erros de alocação de porta

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Alarms (Alarmes), All alarms (Todos os alarmes).
3. Selecione Criar alarme.
4. Escolha Selecionar métrica.
5. Escolha o namespace de métrica NATGateway e, em seguida, escolha uma dimensão de métrica. Quando você chegar às métricas, marque a caixa de seleção ao lado da métrica ErrorPortAllocation para o gateway NAT e, em seguida, escolha Select metric (Selecionar métrica).

6. Configure o alarme como indicado a seguir e, em seguida, selecione Avançar:
   - Em Statistic (Estatística), escolha Maximum (Máximo).
   - Em Period (Período), escolha 5 minutes (5 minutos).
   - Em Whenever (Sempre que), escolha Greater (Maior que) e insira 0 como limite.
   - Em Additional configuration (Configuração adicional), Datapoints to alarm (Pontos de dados para alarme), insira 3.
7. Em Notification (Notificação), escolha um tópico existente do SNS ou Create new topic (Criar tópico) para criar um. Escolha Próximo.
8. Insira um nome e uma descrição para o alarme e selecione Avançar.
9. Quando terminar de configurar o alarme, escolha Create alarm (Criar alarme).

Para obter mais informações, consulte Uso de alarmes do Amazon CloudWatch no Manual do usuário do Amazon CloudWatch.

Solucionar problemas de gateways NAT

Os tópicos a seguir ajudam a solucionar problemas comuns que você pode encontrar ao criar ou usar um gateway NAT.

Problemas

- Falha na criação do gateway NAT
- Cota de gateway NAT
- Cota de endereços IP elásticos
- A zona de disponibilidade é incompatível
- O gateway NAT não está mais visível
- O gateway NAT não responde a um comando ping
- As instâncias não conseguem acessar a Internet
- A conexão TCP para um destino apresenta falha
- O resultado do traceroute não exibe endereço IP privado do gateway NAT
- A conexão com a Internet cai após 350 segundos
- Não é possível estabelecer uma conexão IPsec
- Não é possível iniciar mais conexões

Falha na criação do gateway NAT

Problema

Você cria um gateway NAT e ele entra no status `Failed`.

> **Note**
>
> Um gateway NAT com falha é excluído automaticamente, geralmente em cerca de uma hora.

Causa

Ocorreu um erro quando o gateway NAT foi criado. A mensagem de estado retornada fornece o motivo do erro.

Solução

Para visualizar a mensagem de erro, abra o console da Amazon VPC e selecione NAT Gateways (Gateways NAT). Selecione o botão de opção do gateway NAT e, em seguida, encontre a State message (Mensagem de estado) na guia Details (Detalhes).

A tabela a seguir lista as possíveis causas da falha, tal como indicado no console da Amazon VPC. Depois de usar quaisquer etapas de correção indicadas, você pode tentar criar o gateway NAT novamente.

Erro exibido	Causa	Solução
Subnet has insufficient free addresses to create this NAT gateway	A sub-rede que você especific ou não tem nenhum endereço IP privado disponível. O gateway NAT requer uma interface de rede com endereço IP privado alocado no intervalo da sub-rede.	Verifique quantos endereços IP estão disponíveis na sub-rede acessando a página Subnets (Sub-redes) no console da Amazon VPC. Você pode visualizar os Available IPs (IPs disponíveis) no painel de detalhes da sub-rede. Para criar endereços IP livres em sua sub-rede, você pode excluir interface s de rede não usadas ou

Erro exibido	Causa	Solução
		encerrar instâncias das quais não necessita.
Network vpc-xxxxxxxx has no Internet gateway attached	É necessário criar um gateway NAT em uma VPC com um gateway da internet.	Crie e vincule um gateway da Internet à VPC. Para ter mais informações, consulte Adicionar acesso à Internet a uma sub-rede.
Elastic IP address eipalloc-xxxxxxxx is already associated	O endereço IP elástico que você especificou já está associado a outro recurso e não pode ser associado ao gateway NAT.	Verifique qual recurso está associado ao endereço IP elástico. Acesse a página Elastic IPs (IPs elásticos) no console da Amazon VPC e visualize os valores especific ados para o ID da instância ou para o ID da interface de rede. Se você não precisar do endereço IP elástico para aquele recurso, poderá dissociá-lo. Outra opção é alocar um novo endereço IP elástico à sua conta. Para ter mais informações, consulte Começar a usar endereços IP elásticos.

Cota de gateway NAT

Ao tentar criar um gateway NAT, você obtém o erro a seguir.

```
Performing this operation would exceed the limit of 5 NAT gateways
```

Causa

Você atingiu a cota do número de gateways NAT para essa zona de disponibilidade.

Solução

Se você atingiu essa cota de gateway NAT para sua conta, você pode fazer um dos seguintes procedimentos:

- Solicite um aumento nos gateways NAT por cota de zona de disponibilidade usando o console Service Quotas.
- Verifique o status de seu gateway NAT. O status `Pending`, `Available` ou `Deleting` é contado em relação à sua cota. Se você tiver excluído um gateway NAT recentemente, espere alguns minutos para o status passar de `Deleting` para `Deleted`. Depois, tente criar outro gateway NAT.
- Se não precisar de seu gateway NAT em uma zona de disponibilidade específica, tente criar um gateway NAT em uma zona de disponibilidade em que você não tenha atingido sua cota.

Para obter mais informações, consulte Cotas da Amazon VPC.

Cota de endereços IP elásticos

Problema

Quando você tenta alocar um endereço IP elástico para o gateway NAT público, você recebe o seguinte erro:

```
The maximum number of addresses has been reached.
```

Causa

Você atingiu a cota do número de endereços IP elásticos para sua conta para essa Região.

Solução

Se tiver atingido a cota de endereços IP elásticos, você poderá desassociar um endereço IP elástico de outro recurso. Como alternativa, você pode solicitar um aumento na cota Elastic IPs usando o console Service Quotas.

A zona de disponibilidade é incompatível

Problema

Ao tentar criar um gateway NAT, você obtém o seguinte erro: `NotAvailableInZone`.

Causa

Você pode estar tentando criar o gateway NAT em uma zona de disponibilidade restrita, ou seja, uma zona em que nossa capacidade de expandir é restrita.

Solução

Não é possível oferecer suporte a gateways NAT nessas zonas de disponibilidade. Você pode criar um gateway NAT em uma Zona de disponibilidade diferente e usá-lo para sub-redes privadas na zona restringida. Além disso, você pode mover seus recursos para uma zona de disponibilidade irrestrita para que esses recursos e seu gateway NAT fiquem na mesma zona de disponibilidade.

O gateway NAT não está mais visível

Problema

Você criou um gateway NAT, mas ele não está mais visível no console da Amazon VPC.

Causa

Pode ter ocorrido um erro durante a criação do gateway NAT e a criação falhou. Um gateway NAT com um status `Failed` fica visível no console da Amazon VPC por mais ou menos uma hora). Após uma hora, ele é excluído automaticamente.

Solução

Examine as informações em Falha na criação do gateway NAT e tente criar um novo gateway NAT.

O gateway NAT não responde a um comando ping

Problema

Ao tentar executar ping em um endereço IP elástico ou em um endereço IP privado do gateway NAT na internet (por exemplo, no computador doméstico) ou em uma instância na VPC, você não receberá uma resposta.

Causa

O gateway NAT só transfere tráfego de uma instância em uma sub-rede privada para a internet.

Solução

Para testar se um gateway NAT está funcionando, consulte Testar o gateway NAT público.

As instâncias não conseguem acessar a Internet

Problema

Você criou um gateway NAT público e seguiu as etapas para testá-lo, mas o comando `ping` apresenta falha ou suas instâncias da sub-rede privada não conseguem acessar a Internet.

Causas

A causa desse problema pode ser uma das seguintes:

- O gateway NAT não está pronto para enviar tráfego.
- Sua tabela de rotas não está configurada de corretamente.
- Seus grupos de segurança ou network ACLs estão bloqueando o tráfego de entrada ou de saída.
- Você está usando um protocolo incompatível.

Solução

Verifique as seguintes informações:

- Verifique se o gateway NAT encontra-se no estado `Available`. No console da Amazon VPC, acesse a página NAT Gateways (Gateways NAT) e visualize as informações de status no painel de detalhes. Se o gateway NAT estiver no estado de falha, pode ter havido um erro no momento de criá-lo. Para obter mais informações, consulte Falha na criação do gateway NAT.
- Verifique se você configurou corretamente as tabelas de rotas:
  - O gateway NAT deve estar em uma sub-rede pública com uma tabela de rotas que roteia o tráfego da internet para um gateway da internet.
  - A instância deve estar em uma sub-rede privada com uma tabela de rotas que roteia o tráfego da internet para o gateway NAT.
  - Verifique se não existe nenhuma outra entrada na tabela de rotas que roteia todo ou parte do tráfego da internet para outro dispositivo, e não para o gateway NAT.
- Verifique se as regras do security group para a instância privada permitem tráfego de saída pela internet. Para o comando `ping` funcionar, as regras devem também permitir tráfego ICMP de saída.

  O gateway NAT propriamente dite permite tráfego de saída e tráfego recebido em resposta a uma solicitação de saída (por isso, ele é com estado).
- Verifique se as Network ACLs associadas à sub-rede privada e às sub-redes públicas não têm regras que bloqueiam o tráfego de entrada e saída de internet. Para o comando `ping` funcionar, as regras devem também permitir tráfego ICMP de entrada e saída.

Você pode permitir logs de fluxo para ajudá-lo a diagnosticar conexões encerradas por causa de regras de Network ACL ou security group. Para obter mais informações, consulte Como registrar tráfego IP em log com logs de fluxo da VPC.

- Se estiver usando o comando `ping`, verifique se está executando um ping para um host habilitado para ICMP. Se o ICMP não estiver habilitado, você não receberá pacotes de resposta. Para testar, execute o mesmo comando `ping` no terminal de linha de comando de seu computador.
- Verifique se sua instância pode executar ping em outros recursos; por exemplo, outras instâncias na sub-rede privada (supondo que as regras de security group permitam isso).
- Verifique se sua conexão está usando somente o protocolo TCP, UDP ou ICMP.

A conexão TCP para um destino apresenta falha

Problema

Algumas conexões TCP de instâncias em uma sub-rede privada para um destino específico por um gateway NAT são bem-sucedidas, mas outras estão apresentando falha ou atingindo o tempo limite.

Causas

A causa desse problema pode ser uma das seguintes:

- O endpoint de destino está respondendo com pacotes TCP fragmentados. Os gateways NAT não suportam fragmentação de IP para TCP ou ICMP. Para obter mais informações, consulte Comparar gateways NAT e instâncias NAT.
- A opção `tcp_tw_recycle` está habilitada no servidor remoto, que é conhecido por causar problemas quando há várias conexões por trás de um dispositivo NAT.

Soluções

Verifique se o endpoint ao qual você está tentando conectar está respondendo com pacotes TCP fragmentados fazendo o seguinte:

1. Use uma instância em uma sub-rede pública com um endereço IP pública para acionar uma resposta grande o suficiente para causar uma fragmentação de um endpoint específico.
2. Use o utilitário Use the `tcpdump` para verificar se o endpoint está enviando pacotes fragmentados.

> **Important**
>
> É necessário usar uma instância em uma sub-rede pública para executar essas verificações. Não é possível usar a instância na qual a conexão original estava falhando ou uma instância em uma sub-rede privada subjacente a um gateway NAT ou a uma instância NAT.

As ferramentas de diagnóstico que enviam ou recebem grandes pacotes ICMP relatarão perda de pacote. Por exemplo, o comando `ping -s 10000 example.com` não funciona com um gateway NAT.

3. Se o endpoint estiver enviando pacotes TCP fragmentados, você poderá usar uma instância NAT, em vez de um gateway NAT.

Se tiver acesso ao servidor remoto, você poderá verificar se a opção `tcp_tw_recycle` está habilitada fazendo o seguinte:

1. No servidor, execute o comando a seguir.

```
cat /proc/sys/net/ipv4/tcp_tw_recycle
```

Se a saída for 1, a opção `tcp_tw_recycle` estará habilitada.

2. Se a opção `tcp_tw_recycle` estiver habilitada, recomendamos desabilitá-la. Se precisar reutilizar conexões, `tcp_tw_reuse` é uma opção mais segura.

Se não tiver acesso ao servidor remoto, você poderá testar desabilitando temporariamente a opção `tcp_timestamps` em uma instância na sub-rede privada. Depois, conecte ao servidor remoto novamente. Se a conexão for bem-sucedida, a causa da falha anterior provavelmente ocorreu porque `tcp_tw_recycle` está habilitado no servidor remoto. Se for possível, entre em contato com o proprietário do servidor remoto para verificar se essa opção está habilitada e solicite que ela seja desabilitada.

O resultado do traceroute não exibe endereço IP privado do gateway NAT

Problema

A instância pode acessar a internet, mas quando você executa o comando `traceroute`, o resultado não exibe o endereço IP privado do gateway NAT.

Causa

A instância está acessando a internet usando um gateway diferente, como um gateway da Internet.

Solução

Na tabela de rotas da sub-rede na qual sua instância está localizada, verifique as informações a seguir:

- Verifique se existe uma rota que envia tráfego de internet para o gateway NAT.
- Verifique se não existe mais de uma rota específica enviando tráfego de internet para outros dispositivos, como um gateway privado virtual ou um gateway da internet.

A conexão com a Internet cai após 350 segundos

Problema

A instância pode acessar a Internet, mas a conexão cai após 350 segundos.

Causa

Se uma conexão que usa um gateway NAT ficar ociosa por 350 segundos ou mais, ela expirará.

Quando uma conexão atinge o tempo limite, uma gateway NAT retorna um pacote RST a qualquer recurso subjacente ao gateway NAT que tenta dar continuidade à conexão (ele não envia um pacote FIN).

Solução

Para evitar que a conexão caia, você pode iniciar mais tráfegos por meio da conexão. Como alternativa, é possível habilitar o keepalive TCP na instância com um valor menor que 350 segundos.

Não é possível estabelecer uma conexão IPsec

Problema

Não é possível estabelecer uma conexão IPsec em um destino.

Causa

Atualmente, os gateways NAT não são compatíveis com o protocolo IPsec.

Solução

Você pode usar o NAT- Traversal (NAT-T) para encapsular o tráfego IPsec na UDP, que é um protocolo compatível com gateways NAT. Lembre-se de testar sua configuração de NAT-T e de IPsec para verificar se o tráfego IPsec não é interrompido.

Não é possível iniciar mais conexões

Problema

Você tem conexões existentes para um destino por meio de um gateway NAT, mas não pode estabelecer mais conexões.

Causa

Talvez você tenha atingido o limite de conexões simultâneas para um único gateway NAT. Para obter mais informações, consulte Noções básicas de gateway NAT. Se as instâncias na sub-rede privada criarem um grande número de conexões, você poderá atingir esse limite.

Solução

Execute um destes procedimentos:

- Criar um gateway NAT por Zona de disponibilidade e distribuir seus clientes nessas zonas.
- Criar outros gateways NAT na sub-rede pública e distribuir seus clientes em várias sub-redes privadas, cada uma com uma rota para um gateway NAT diferente.
- Limitar o número de conexões que seus clientes podem criar para o destino.
- Use a métrica `IdleTimeoutCount` no CloudWatch para monitorar aumentos nas conexões ociosas. Fechar as conexões ociosas para liberar capacidade.
- Crie um gateway NAT com vários endereços IP ou adicione endereços IP secundários a um gateway NAT existente. Cada novo endereço IPv4 comporta no máximo 55.000 conexões simultâneas. Para obter mais informações, consulte Criar um gateway NAT ou Editar associações de endereço IP secundário.

Preços de gateways NAT

Ao provisionar um gateway NAT, você é cobrado por cada hora que o gateway NAT está disponível e por cada gigabyte de dados que ele processa. Para obter mais informações, consulte Definição de preço da Amazon VPC.

As estratégias a seguir podem ajudar você a reduzir as cobranças de transferência de dados para o gateway NAT:

- Se seus recursos da AWS enviam ou recebem um volume significativo de tráfego entre zonas de disponibilidade, certifique-se de que os recursos estejam na mesma zona de disponibilidade que o gateway NAT. Como alternativa, crie um gateway NAT em cada zona de disponibilidade com recursos.
- Se a maior parte do tráfego através do gateway NAT for para serviços AWS compatíveis com endpoints de interface ou endpoints de gateway, considere a criação de um endpoint de interface ou endpoint de gateway para esses serviços. Para obter mais informações sobre as possíveis economias de custo, consulte AWS PrivateLink Preço.

Instâncias NAT

Uma instância NAT fornece conversão de endereços de rede (NAT). É possível usar uma instância NAT para permitir que recursos em uma sub-rede privada se comuniquem com destinos fora da nuvem privada virtual (VPC), como a Internet ou uma rede on-premises. Os recursos na sub-rede privada podem iniciar o tráfego IPv4 de saída para a Internet, mas não podem receber o tráfego de entrada iniciado na Internet.

> **Important**
>
> A AMI de NAT é construída com base na última versão do Amazon Linux, 2018.03, que atingiu o final do ciclo de suporte padrão em 31 de dezembro de 2020 e o final do ciclo de suporte de manutenção em 31 de dezembro de 2023. Para obter mais informações, consulte a seguinte postagem no blog: Amazon Linux AMI end of life.
> Se você usar uma AMI de NAT existente, a AWS recomenda migrar para um gateway NAT. Os gateways NAT oferecem maior disponibilidade e maior largura de banda e exigem menos esforços administrativos. Para ter mais informações, consulte Comparar gateways NAT e instâncias NAT.
> Se as instâncias de NAT forem uma correspondência melhor para o seu caso de uso do que os gateways NAT, você poderá criar sua própria AMI de NAT com base em uma versão atual do Amazon Linux conforme descrita em the section called “3. Crie uma AMI de NAT”.

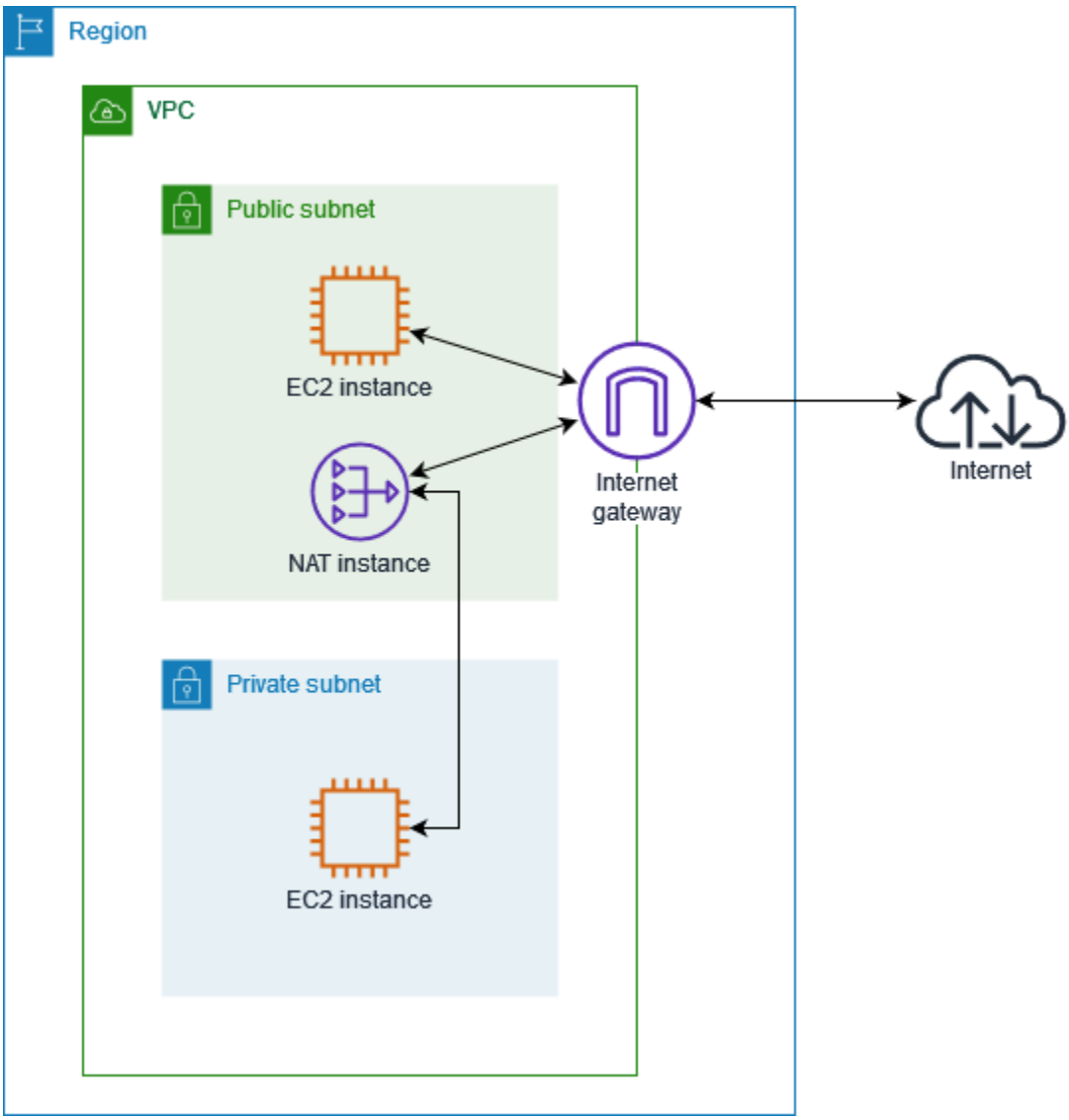
Conteúdo

- Permitir que recursos privados se comuniquem fora da VPC

Noções básicas sobre a instância NAT

A figura a seguir mostra noções básicas sobre instância NAT. A tabela de rotas associada à sub-rede privada envia o tráfego da Internet das instâncias na sub-rede privada para a instância NAT na sub-rede pública. Em seguida, a instância NAT envia o tráfego para o gateway da Internet. O tráfego é atribuído ao endereço IP público da instância NAT. A instância NAT especifica um número de porta alto para a resposta; quando uma resposta retorna, a instância NAT a envia a uma instância na sub-rede privada com base no número da porta para a resposta.

A instância NAT deve ter acesso à Internet, portanto, deve estar em uma sub-rede pública (uma sub-rede que possui uma tabela de rotas com uma rota para o gateway da Internet) e deve ter um endereço IP público ou um endereço IP elástico.



Para começar a usar instâncias NAT, crie uma AMI de NAT, crie um grupo de segurança para a instância NAT e execute a instância NAT em sua VPC.

Sua cota de instância NAT depende da cota de instância para a região. Para obter mais informações, consulte Service Quotas do Amazon EC2 na Referência geral da AWS.

Permitir que recursos privados se comuniquem fora da VPC

Esta seção descreve como criar e trabalhar com instâncias NAT para permitir que recursos em uma sub-rede privada se comuniquem fora da nuvem privada virtual.

Tarefas

- 1. Crie uma VPC para a instância NAT

1. Crie uma VPC para a instância NAT

Use o procedimento a seguir para criar uma VPC com uma sub-rede pública e uma sub-rede privada.

Como criar a VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. Escolha Criar VPC.
3. Em Resources to create (Recursos a serem criados), escolha VPC and more (VPC e mais).
4. Em Name tag auto-generation (Geração automática de tags de nome), insira um nome para a VPC.
5. Para configurar as sub-redes, faça o seguinte:
    a. Em Number of Availability Zones (Número de zonas de disponibilidade), escolha 1 ou 2 dependendo das suas necessidades.
    b. Em Number of public subnets (Número de sub-redes públicas), verifique se você tem uma sub-rede pública por zona de disponibilidade.
    c. Em Number of private subnets (Número de sub-redes privadas), verifique se você tem uma sub-rede privada por zona de disponibilidade.
6. Escolha Criar VPC.

2. Crie um grupo de segurança para a instância NAT

Crie um grupo de segurança com as regras descritas na tabela a seguir. Essas regras possibilitam que sua instância NAT receba tráfego vinculado à Internet de instâncias na sub-rede privada, bem como tráfego SSH de sua rede. A instância NAT também pode enviar tráfego à Internet, o que permite que as instâncias na sub-rede privada obtenham atualizações de software.

As regras recomendadas de entrada são mostradas a seguir.

Origem	Protocolo	Intervalo de portas	Comentários
CIDR da sub-rede privada	TCP	80	Permite tráfego HTTP de entrada de servidores na sub-rede privada.
CIDR da sub-rede privada	TCP	443	Permite tráfego HTTPS de entrada de servidores na sub-rede privada.
Intervalo de endereços IP públicos da sua rede	TCP	22	Permitir acesso SSH de entrada de sua rede à instância NAT (por meio do gateway da Internet).

As regras recomendadas de saída são mostradas a seguir.

Destino	Protocolo	Intervalo de portas	Comentários
0.0.0.0/0	TCP	80	Permite acesso HTTP de saída à Internet.
0.0.0.0/0	TCP	443	Permite acesso HTTPS de saída à Internet.

Como criar o grupo de segurança

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Grupos de segurança.
3. Escolha Create grupo de segurança (Criar grupo de segurança).
4. Insira um nome e uma descrição para o grupo de segurança.
5. Em VPC, selecione o ID da VPC para sua instância NAT.
6. Adicione regras para o tráfego de entrada em Regras de entrada da seguinte forma:

a. Escolha Adicionar regra. Escolha HTTP em Tipo e insira o intervalo de endereços IP de sua sub-rede privada em Fonte.

b. Escolha Adicionar regra. Escolha HTTPS em Tipo e insira o intervalo de endereços IP de sua sub-rede privada em Fonte.

c. Escolha Adicionar regra. Escolha SSH em Tipo e insira o intervalo de endereços IP da sua rede em Fonte.

7. Adicione regras para o tráfego de saída em Regras de saída da seguinte forma:

a. Escolha Adicionar regra. Escolha HTTP em Tipo e digite 0.0.0.0/0 em Destino.

b. Escolha Adicionar regra. Escolha HTTPS em Tipo e digite 0.0.0.0/0 em Destino.

8. Escolha Create security group (Criar grupo de segurança).

Para ter mais informações, consulte Grupos de segurança.

3. Crie uma AMI de NAT

Uma AMI de NAT é configurada para executar NAT em uma instância do EC2. Você deve criar uma AMI de NAT e, em seguida, executar sua instância NAT usando a AMI de NAT.

Caso planeje usar um sistema operacional diferente do Amazon Linux para sua AMI de NAT, consulte a documentação desse sistema operacional para saber como configurar a NAT. Não se esqueça de salvar essas configurações para que elas persistam mesmo após a reinicialização da instância.

Criar uma AMI de NAT para o Amazon Linux

1. Inicie uma instância do EC2 executando o AL2023 ou o Amazon Linux 2. Não deixe de especificar o grupo de segurança que você criou para a instância do NAT.
2. Conecte-se à sua instância e execute os comandos a seguir na instância para habilitar iptables.

```
sudo yum install iptables-services -y
sudo systemctl enable iptables
sudo systemctl start iptables
```

3. Faça o seguinte na instância para habilitar o encaminhamento de IP de forma que ele persista após a reinicialização:

a. Usando um editor de texto, como nano ou vim, crie um arquivo com a seguinte configuração: `/etc/sysctl.d/custom-ip-forwarding.conf`.

b. Adicione a seguinte linha ao arquivo de configuração.

```
net.ipv4.ip_forward=1
```

c. Salve o arquivo de configuração e saia do editor de texto.

d. Execute o comando a seguir para aplicar o arquivo de configuração.

```
sudo sysctl -p /etc/sysctl.d/custom-ip-forwarding.conf
```

4. Execute o comando a seguir na instância e anote o nome da interface de rede primária. Você precisará dessas informações para a próxima etapa.

```
netstat -i
```

No exemplo de saída a seguir, `docker0` é uma interface de rede criada pelo docker, `eth0` é a interface de rede primária e `lo` é a interface de loopback.

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
docker0   1500        0      0      0 0             0      0      0      0 BMU
eth0      9001  7276052      0      0 0       5364991      0      0      0 BMRU
lo       65536   538857      0      0 0        538857      0      0      0 LRU
```

No exemplo de saída a seguir, a interface de rede primária é `enX0`.

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enX0      9001     1076      0      0 0          1247      0      0      0 BMRU
lo       65536       24      0      0 0            24      0      0      0 LRU
```

No exemplo de saída a seguir, a interface de rede primária é `ens5`.

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
ens5      9001    14036      0      0 0          2116      0      0      0 BMRU
lo       65536       12      0      0 0            12      0      0      0 LRU
```

5. Execute os comandos a seguir na instância para configurar o NAT. Se a interface de rede primária não for `eth0`, substitua *`eth0`* pela interface de rede primária indicada na etapa anterior.

```
sudo /sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
sudo /sbin/iptables -F FORWARD
sudo service iptables save
```

6. Crie uma AMI de NAT da instância do EC2. Para obter mais informações, consulte Criar uma AMI do Linux a partir de uma instância no Guiado usuário do Amazon EC2.

4. Execute uma instância NAT

Use o procedimento a seguir para executar uma instância NAT usando a VPC, o grupo de segurança e a AMI de NAT que você criou.

Executar uma instância NAT

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel, escolha Executar instância.
3. Em Nome, insira um nome para sua instância NAT.
4. Em Aplicações e imagens do SO, selecione sua AMI de NAT (escolha Procurar mais AMIs e Minhas AMIs).
5. Em Tipo de instância, escolha um tipo de instância que forneça os recursos de computação, memória e armazenamento de que sua instância NAT precisa.
6. Em Par de chaves, selecione um par de chaves existente ou escolha Criar novo par de chaves.
7. Em Configurações de rede, faça o seguinte:
   a. Escolha Editar.
   b. Em VPC, escolha a VPC criada anteriormente.
   c. Em Sub-rede, selecione a sub-rede pública criada anteriormente para a VPC.
   d. Em Atribuir IP público automaticamente, selecione Habilitar. Como alternativa, após executar a instância NAT, aloque um endereço IP elástico e atribua-o à instância NAT.
   e. Em Firewall, escolha Selecionar grupo de segurança existente e, em seguida, escolha o grupo de segurança que você criou.
8. Escolha Iniciar instância. Escolha o ID da instância para abrir a página de detalhes da instância. Aguarde o estado da instância mudar para Em execução, bem como a conclusão bem-sucedida das verificações de status.

9. Desabilite as verificações de origem e destino para a instância NAT (consulte 5. Desativar as verificações de origem/destino).
10. Atualize a tabela de rotas para enviar tráfego para a instância NAT (consulte 6. Atualize a tabela de rotas).

5. Desativar as verificações de origem/destino

Por padrão, toda Instância EC2 executa verificações origem/destino. Isso significa que a instância deve ser a origem ou o destino de qualquer tráfego que ela envia ou recebe. Entretanto, a instância NAT deve poder enviar e receber tráfego quando ela não é a origem nem o destino. Por isso, você deve desativar as verificações de origem/destino na instância NAT.

Desabilitar as verificações de origem e destino

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância NAT.
4. Escolha Ações, Redes, Alterar verificação de origem/destino.
5. Em Verificação de origem e destino, selecione Interromper.
6. Escolha Save (Salvar).
7. Se a instância NAT tem uma interface de rede secundária, escolha-a em Network interfaces (Interfaces de rede) na guia Networking (Rede) guia. Escolha a interface ID para ir à página das interfaces de rede. Selecione Actions (Ações), Change source/dest. check (Alterar verificação de origem/destino), desmarque Enable (Habilitar) e selecione Save (Salvar).

6. Atualize a tabela de rotas

A tabela de rotas para a sub-rede privada deve ter uma rota que envie o tráfego da Internet para a instância NAT.

Atualizar a tabela de rotas

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Route tables.
3. Selecione a tabela de rotas para a sub-rede privada.
4. Na guia Rotas, escolha Editar rotas e, em seguida, escolha Adicionar rota.

5. Insira 0.0.0.0/0 para Destino e o ID da instância NAT para Alvo.
6. Escolha Salvar alterações.

Para ter mais informações, consulte Configurar tabelas de rotas.

7. Teste sua instância NAT

Após executar uma instância NAT e concluir as etapas anteriores de configuração, você pode testar se uma instância em sua sub-rede privada pode acessar a Internet por meio da instância NAT ao usar a instância NAT como um servidor bastion.

Tarefas

- Etapa 1: atualizar o grupo de segurança da instância NAT
- Etapa 2: inicie uma instância de teste na sub-rede privada
- Etapa 3: efetuar ping em um site habilitado para ICMP
- Etapa 4: limpar

Etapa 1: atualizar o grupo de segurança da instância NAT

Para permitir que as instâncias na sua sub-rede privada enviem tráfego de ping à instância NAT, adicione uma regra para permitir tráfego ICMP de entrada e saída. Para permitir que a instância NAT atue como servidor bastion, adicione uma regra para permitir o tráfego SSH de saída para a sub-rede privada.

Atualizar o grupo de segurança da instância NAT

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Grupos de segurança.
3. Marque a caixa de seleção do grupo de segurança associado à sua instância NAT.
4. Na guia Regras de entrada, selecione Editar regras de entrada.
5. Escolha Add rule (Adicionar regra). Escolha All ICMP - IPv4 (Todos ICMP - IPv4) para Type (Tipo). Escolha Personalizar em Fonte e insira o intervalo de endereços IP de sua sub-rede privada. Selecione Salvar rules.
6. Na guia Regras de saída, escolha Editar regras de saída.
7. Escolha Add rule (Adicionar regra). Escolha SSH para Type (Tipo) . Escolha Personalizar em Destino e insira o intervalo de endereços IP de sua sub-rede privada.

8. Escolha Add rule (Adicionar regra). Escolha All ICMP - IPv4 (Todos ICMP - IPv4) para Type (Tipo). Escolha Anywhere - IPv4 (Em qualquer lugar - IPv4) em Destination (Destino). Escolha Save rules (Salvar regras).

Etapa 2: inicie uma instância de teste na sub-rede privada

Execute uma instância em sua sub-rede privada. Você deve permitir o acesso SSH da instância NAT e usar o mesmo par de chaves usado para a instância NAT.

Iniciar uma instância de teste na sub-rede privada

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel, escolha Executar instância.
3. Selecione sua sub-rede privada.
4. Não atribua um endereço IP público a esta instância.
5. Certifique-se de que o grupo de segurança para esta instância permita acesso SSH de entrada de sua instância NAT ou do intervalo de endereços IP de sua sub-rede pública e tráfego ICMP de saída.
6. Selecione o mesmo par de chaves usado para a instância NAT.

Etapa 3: efetuar ping em um site habilitado para ICMP

Para verificar se a instância de teste na sub-rede privada pode usar a instância NAT para se comunicar com a Internet, execute o comando ping.

Testar a conexão com a Internet de sua instância privada

1. No computador local, configure o encaminhamento de agentes SSH, para poder usar a instância NAT como um servidor bastion.

   Linux and macOS

   ```
   ssh-add key.pem
   ```

   Windows

   Baixe e instale o Pageant, se ainda não estiver instalado.

Converta a chave privada usando o PuTTYgen.

Inicie o Pageant, clique com o botão direito no ícone do Pageant na barra de tarefas (ele pode estar oculto) e escolha Adicionar chave. Selecione o arquivo .ppk que você criou, insira a senha se necessário e escolha Abrir.

2. No computador local, conecte-se à sua instância do NAT.

   Linux and macOS

   ```
   ssh -A ec2-user@nat-instance-public-ip-address
   ```

   Windows

   Conectar-se à sua instância do NAT do usando o PuTTY. Para Autenticação, você deve selecionar Permitir encaminhamento de agentes e deixar a opção Arquivo de chave privada para autenticação em branco.

3. Na instância NAT, execute o comando ping, especificando um site que está habilitado para ICMP.

   ```
   [ec2-user@ip-10-0-4-184]$ ping ietf.org
   ```

   Para confirmar que sua instância NAT tem acesso à Internet, verifique se você recebeu uma saída como a seguinte e pressione Ctrl+C para cancelar o comando ping. Caso contrário, verifique se a instância NAT está em uma sub-rede pública (sua tabela de rotas tem uma rota para um gateway da Internet).

   ```
   PING ietf.org (104.16.45.99) 56(84) bytes of data.
   64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=1 ttl=33 time=7.88 ms
   64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=2 ttl=33 time=8.09 ms
   64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=3 ttl=33 time=7.97 ms
   ...
   ```

4. Em sua instância NAT, conecte-se à instância em sua sub-rede privada ao usar o respectivo endereço IP privado.

   ```
   [ec2-user@ip-10-0-4-184]$ ssh ec2-user@private-server-private-ip-address
   ```

5. Em sua instância privada, teste se você pode se conectar à Internet ao executar o comando ping.

```
[ec2-user@ip-10-0-135-25]$ ping ietf.org
```

Para confirmar que sua instância privada tem acesso à Internet por meio da instância NAT, verifique se você recebeu uma saída como a seguinte e pressione Ctrl+C para cancelar o comando ping.

```
PING ietf.org (104.16.45.99) 56(84) bytes of data.
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=1 ttl=33 time=8.76 ms
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=2 ttl=33 time=8.26 ms
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=3 ttl=33 time=8.27 ms
...
```

Solução de problemas

Se o comando ping falhar no servidor na sub-rede privada, use as seguintes etapas para solucionar o problema:

- Verifique se você usou o comando ping em um site habilitado para ICMP. Caso contrário, seu servidor não poderá receber pacotes de resposta. Para testar isso, execute o mesmo comando ping em um terminal de linha de comando em seu computador.
- Verifique se o grupo de segurança para sua instância NAT permite tráfego ICMP de entrada de sua sub-rede privada. Caso contrário, sua instância NAT não poderá receber o comando ping de sua instância privada.
- Verifique se você desabilitou a verificação de origem e destino para sua instância NAT. Para ter mais informações, consulte 5. Desativar as verificações de origem/destino.
- Verifique se você configurou suas tabelas de rota corretamente. Para ter mais informações, consulte 6. Atualize a tabela de rotas.

Etapa 4: limpar

Se você não precisar mais do servidor de teste na sub-rede privada, encerre a instância para que ela não gere mais cobranças. Para obter mais informações, consulte Terminar sua instância no Guia do usuário do Amazon EC2.

Se você não precisar mais da instância NAT, poderá interrompê-la ou encerrá-la para não gerar mais cobranças. Se você criou uma AMI NAT, pode criar uma nova instância NAT sempre que precisar de uma.

Comparar gateways NAT e instâncias NAT

O resumo a seguir detalha as diferenças entre gateways NAT e instâncias NAT. Recomendamos usar gateways NAT porque eles fornecem melhor disponibilidade e largura de banda e exigem menos esforço para administrar.

Atributo	gateway NAT	Instância do NAT
Disponibilidade	Altamente disponível. Em cada Zona de disponibilidade são implementados gateways NAT com redundância. Crie um gateway NAT em cada Zona de disponibilidade para assegurar uma arquitetura independente de zona.	Use um script para gerenciar o failover entre as instâncias.
Largura de banda	Escalabilidade de até 100 Gbps.	Depende da largura de banca do tipo da instância.
Manutenção	Gerenciado pela AWS. Não há necessidade de realizar manutenção.	Gerenciada por você. Por exemplo, instalação de atualizações de software ou patches de sistema operacional na instância.
Performance	O software é otimizado por meio do gerenciamento do tráfego NAT.	Uma AMI genérica que é configurada para desempenhar a tarefa de NAT.
Custos	A cobrança depende do número de gateways NAT que você usar, do tempo de uso e da quantidade de dados enviados por meio dos gateways NAT.	A cobrança depende do número de instâncias NAT que você usar, do tempo de uso e do tipo e tamanho da instância.

Atributo	gateway NAT	Instância do NAT
Tipo e tamanho	Produto invariável; não há necessidade de tomar decisões sobre tipo nem tamanho.	Escolha um tipo e tamanho adequados de instância de acordo com sua previsão de workload.
Endereços IP públicos	Escolha o endereço IP elástico para associar a um gateway NAT público no momento da criação.	Use um endereço IP elástico ou um endereço IP público com uma instância NAT. Você pode alterar o endereço IP público a qualquer momento associando um novo endereço IP elástico à instância.
Endereços IP privados	Selecionados automaticamente no intervalo de endereços IP da sub-rede quando você cria o gateway.	Atribua um endereço IP privado específico do intervalo de endereços IP da sub-rede quando você executar a instância.
Grupos de segurança	Não é possível associar grupos de segurança a gateways NAT. Você pode associá-los aos seus recursos por trás do gateway NAT para controlar o tráfego de entrada e de saída.	Associe à sua instância NAT e aos recursos subjacentes à sua instância NAT para controlar o tráfego de entrada e de saída.
Network ACLs	Use uma Network ACL para controlar o tráfego para e proveniente da sub-rede na qual seu gateway NAT reside.	Use uma Network ACL para controlar o tráfego para e proveniente da sub-rede na qual instância NAT reside.
Logs de fluxo	Use logs de fluxo para capturar o tráfego.	Use logs de fluxo para capturar o tráfego.
Encaminhamento de portas	Não compatível.	Personalize manualmente a configuração para comportar encaminhamento de portas.

Atributo	gateway NAT	Instância do NAT
Servidores bastion	Não compatível.	Use um servidores bastion.
Métricas de tráfego	Veja as métricas do CloudWatch para o gateway NAT.	Visualize as métricas do CloudWatch para a instância.
Comportamento do tempo limite	Quando uma conexão atinge o tempo limite, uma gateway NAT retorna um pacote RST a qualquer recurso subjacente e ao gateway NAT que tenta dar continuidade à conexão (ele não envia um pacote FIN).	Quando uma conexão atinge o tempo limite, uma instância NAT envia um pacote FIN a qualquer recurso subjacente e à instância NAT para encerrar a conexão.
Fragmentação de IP	Comporta encaminhamento de pacotes fragmentados de IP para o protocolo UDP. Não comporta fragmentação para os protocolos TCP e ICMP. Os pacotes fragmentados para esses protocolos são interrompidos.	Comporta remontagem de pacotes of IP fragmentados para os protocolos UDP, TCP e ICMP.

Migrar de uma instância NAT para um gateway NAT

Se você já usa uma instância NAT, reomendamos substituí-la por um gateway NAT. Você pode criar um gateway NAT na mesma sub-rede da sua instância NAT e substituir a rota existente em sua tabela de rotas que aponta para a instância NAT por uma rota que aponta para o gateway NAT. Para usar o mesmo endereço IP elástico para o gateway NAT usado no momento para a instância NAT, primeiro é necessário desassociar o endereço IP elástico da instância NAT e associá-lo a seu gateway NAT ao criar o gateway.

Se mudar o roteamento de uma instância NAT para um gateway NAT ou se dissociar o endereço IP elástico de sua instância NAT, qualquer conexão atual será interrompida e precisará ser restabelecida. Verifique se não há nenhuma tarefa essencial em execução (ou qualquer tarefa que seja executada por meio de uma instância NAT).

Associar endereços de IP elásticos a recursos em sua VPC

Um endereço IP elástico é um endereço IPv4 público estático desenvolvido especificamente para a natureza dinâmica da computação em nuvem. Esse recurso permite associar um endereço IP elástico a qualquer instância ou interface de rede em qualquer nuvem privada virtual (VPC) em sua conta da AWS. Ao utilizar endereços IP elásticos, você pode desbloquear uma série de benefícios que simplificam o gerenciamento e a resiliência de sua infraestrutura baseada em nuvem.

Uma das principais vantagens dos endereços IP elásticos é a capacidade de mascarar a falha de uma instância. Caso uma instância sofra uma interrupção inesperada ou precise ser substituída, o endereço IP elástico associado poderá ser remapeado em outra instância em sua VPC. Esse processo de failover garante que suas aplicações e serviços mantenham um endpoint público consistente e confiável, minimizando o tempo de inatividade e proporcionando uma experiência de usuário superior.

Além disso, os endereços IP elásticos oferecem flexibilidade na forma como você gerencia seus recursos de rede. É possível associar e desassociar programaticamente esses endereços conforme necessário, permitindo direcionar o tráfego para diferentes instâncias com base em seus requisitos comerciais em evolução. Essa alocação dinâmica de endereços IP públicos permite que você se adapte às mudanças na demanda, escale sua infraestrutura e implemente arquiteturas inovadoras sem as restrições das atribuições de IP estático.

Além do uso, por exemplo, de failover, os endereços IP elásticos também podem servir como identificadores estáveis para seus recursos baseados na nuvem. Isso pode ser benéfico ao configurar serviços externos, como registros DNS ou regras de firewall, para se comunicar com suas aplicações hospedadas na AWS. Ao associar um endereço IP público persistente, você pode preparar suas configurações de rede para o futuro e evitar a necessidade de atualizar referências externas quando as instâncias subjacentes são substituídas ou escaladas.

Conteúdo

Conceitos e regras de endereço IP elástico

Para usar um endereço IP elástico, primeiro aloque-o para uso na conta. Depois, é possível associá-lo a uma instância ou interface de rede em sua VPC. O endereço IP elástico permanece alocado à sua conta da AWS até você liberá-lo explicitamente.

O endereço IP elástico é uma propriedade de uma interface de rede. Você pode associar um endereço IP elástico a uma instância atualizando a interface de rede anexada à instância. A vantagem de associar o endereço IP elástico a uma interface de rede, em vez de diretamente à instância, é que é possível mover todos os atributos da interface de rede de uma instância para outra em uma única etapa. Para obter mais informações, consulte Interfaces de rede elástica no Guia do usuário do Amazon EC2.

As seguintes regras se aplicam:

- Um endereço IP elástico pode ser associado a uma única instância ou interface de rede por vez.
- É possível mover um endereço IP elástico de uma instância ou interface de rede para outra.
- Se você associar um endereço IP elástico à interface de rede principal de sua instância, o endereço IPv4 público atual (se houver um) será liberado ao grupo de endereços IP públicos. Se você desassociar o endereço IP elástico, a interface de rede principal será automaticamente atribuída a um novo endereço IPv4 público dentro de alguns minutos. Isso não se aplica se você tiver anexado uma segunda interface de rede à sua instância.
- Você tem o limite de cinco endereços IP elásticos. Para ajudar a conservá-los, é possível usar um dispositivo NAT. Para obter mais informações, consulte Estabelecer conexão com a Internet ou a outras redes usando dispositivos NAT.
- Endereços IP elásticos para IPv6 não são compatíveis.
- É possível aplicar uma tag em um endereço IP elástico que é alocado para uso na VPC. No entanto, as tags de alocação de custo não são compatíveis. Se você recupera um endereço IP elástico, as tags não são recuperadas.
- É possível acessar um endereço IP elástico da Internet quando o grupo de segurança e a ACL da rede permitirem tráfego do endereço IP de origem. O tráfego de resposta de dentro da VPC de volta para a Internet requer um gateway da Internet. Para ter mais informações, consulte Grupos de segurança e Network ACLs.
- Use qualquer uma das seguintes opções para os endereços IP elásticos:
  - Peça à Amazon para fornecer os endereços IP elásticos. Ao selecionar essa opção, você poderá associar os endereços IP elásticos a um grupo de borda de rede. Esse é o local a partir do qual anunciamos o bloco CIDR. Definir o grupo de borda de rede limita o bloco CIDR a esse grupo.
  - Use seus próprios endereços IP. Para obter informações sobre como trazer seus próprios endereços IP, consulte Traga seus próprios endereços IP (BYOIP) no Guia do usuário do Amazon EC2.

- Endereços IPv4 públicos são compatíveis com tags de alocação de custos. Caso aplique tags a endereços IP elásticos, você poderá usá-las para rastrear os custos de endereços IPv4 públicos no AWS Cost Explorer.

  Antes de usar tags como tags de alocação de custos, você precisa ativá-las. Para mais informações, consulte Ativar etiquetas de alocação de custos definidas pelo usuário no Guia do usuário do AWS Billing. Observe que depois de criar e aplicar tags definidas pelo usuário aos recursos, pode levar até 24 horas para que as chaves de tags apareçam na página de tags de alocação de custos para ativação.

  Depois que as tags de alocação de custos estiverem ativadas…

  - Para todos os endereços IPv4 públicos (incluindo endereços IPv4 públicos atribuídos a instâncias do EC2 e endereços IP elásticos) associados a uma interface de rede elástica, você pode visualizar os custos associados aos endereços IPv4 públicos no Explorador de Custos escolhendo Tipo de uso > PublicIPv4InUseAddress (Hrs).
  - Se um endereço IP elástico marcado não estiver associado a uma ENI, ou se estiver associado a um recurso interrompido (como uma instância do EC2 parada), ele será considerado um endereço IPv4 ocioso. Você pode visualizar os custos associados a endereços IPv4 ociosos no Explorador de Custos escolhendo Tipo de uso > PublicIPv4IdleAddress (Hrs).

  Para obter mais informações sobre o Explorador de Custos, consulte Analyzing your costs with AWS Cost Explorer no Guia de usuário do AWS Billing.

Os endereços IP elásticos são regionais. Para obter mais informações sobre como usar o Global Accelerator para provisionar endereços IP globais, consulte Usar endereços IP estáticos globais em vez de endereços IP estáticos regionais no Guia do desenvolvedor do AWS Global Accelerator.

Para obter mais informações sobre preços de endereços IP elásticos, consulte Endereço IPv4 público em Preços da Amazon VPC.

Começar a usar endereços IP elásticos

As seções a seguir descrevem como começar a trabalhar com endereços IP elásticos.

Tarefas

- 1. Alocar um endereço IP elástico
- 2. Associar um endereço IP elástico
- 3. Dissociar um endereço IP elástico

- 4. Transferir endereços IP elásticos
- 5. Liberar um endereço IP elástico
- 6. Recuperar um endereço IP elástico
- Visão geral da linha de comando

1. Alocar um endereço IP elástico

Antes de usar um IP elástico, é necessário alocar um para uso em sua VPC.

Para alocar um endereço IP elástico

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Elastic IPs (IPs elásticos)
3. Escolha Alocar endereço IP elástico.
4. (Opcional) Ao alocar um endereço IP elástico (EIP), você escolhe o Grupo de borda de rede no qual alocar o EIP. Um grupo de bordas de rede é uma coleção de zonas de disponibilidade (AZs), das AWS quais a anuncia um endereço IP público. As Zonas Locais (Local Zones) e Zonas Wavelength (Wavelength Zones) podem ter grupos de fronteira de rede diferentes das Zonas de Disponibilidade (AZs) em uma Região para garantir a latência mínima ou distância física entre a rede AWS e os clientes que acessam os recursos nessas Zonas.

   > **Important**
   >
   > Você deve alocar um EIP no mesmo grupo de fronteiras de rede do AWS recurso que será associado ao EIP. Um EIP (Endereço IP Elástico) em um grupo de fronteira de rede só pode ser anunciado em zonas dentro desse grupo de fronteira de rede e não em nenhuma outra zona representada por outros grupos de fronteira de rede.

   Se você tiver Zonas Locais ou Zonas de Comprimento de Wavelength ativadas (para obter mais informações, consulte Habilitar uma Zona Local ou Ativar zonas de comprimento de onda), você pode escolher um grupo de borda de rede para AZs, Zonas Locais ou Zonas de Comprimento de Onda. Escolha o grupo de bordas de rede com cuidado, pois o EIP e o AWS recurso ao qual ele está associado devem residir no mesmo grupo de bordas de rede. Você pode usar o console do EC2 para visualizar o grupo de fronteiras de rede em que suas zonas de disponibilidade, zonas locais ou zonas de comprimento de onda estão (consulte Zonas Locais). Normalmente, todas

as zonas de disponibilidade em uma região pertencem ao mesmo grupo de fronteiras de rede, enquanto as zonas locais ou zonas de comprimento de onda pertencem a seus próprios grupos de fronteiras de rede separados.

Se você não tiver zonas locais ou zonas de comprimento de onda habilitadas, ao alocar um EIP, o grupo de bordas de rede que representa todas as AZs da região (como `us-west-2`) será predefinido para você e não será possível alterá-lo. Isso significa que o EIP alocado para esse grupo de borda de rede será anunciado em todas as AZs da região em que você está.

5. Em Public IPv4 address pool (Grupo de endereços IPv4 público), escolha uma das seguintes opções:

   - Amazon's pool of IP addresses (Grupo de endereços IP da Amazon): se você quiser que um endereço IPv4 seja alocado do grupo de endereços IP da Amazon.
   - My pool of public IPv4 addresses (Meu grupo de endereços IPv4 públicos): se você deseja alocar um endereço IPv4 a partir de um grupo de endereços IP que trouxe para sua conta da AWS. Essa opção será desabilitada se você não tiver nenhum pool de endereços IP.
   - Customer owned pool of IPv4 addresses (Grupo de endereços IPv4 de propriedade do cliente) se você quiser alocar um endereço IPv4 de um grupo criado a partir de sua rede on-premises para uso com um Outpost. Essa opção não estará disponível se você não tiver um Outpost.

6. (Opcional) Adicione ou remova uma tag.

   [Adicionar uma tag] Escolha Adicionar nova tag e faça o seguinte:

   - Em Chave, insira o nome da chave.
   - Em Value (Valor), insira o valor da chave.

   [Remover uma tag] Escolha Remover à direita da chave e do valor da tag.

7. Escolha Allocate.

2. Associar um endereço IP elástico

É possível associar um IP elástico a uma instância em execução ou interface de rede em sua VPC.

Assim que associar o endereço IP elástico à sua instância, ela receberá um nome de host de DNS público, se os nomes de host de DNS estiverem habilitados. Para obter mais informações, consulte Atributos de DNS para sua VPC.

Como associar um endereço IP elástico a uma instância ou interface de rede

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Elastic IPs (IPs elásticos)
3. Selecione um endereço IP elástico alocado para ser usado com uma VPC (a coluna Scope (Escopo) tem o valor `vpc`) e escolha Actions (Ações) e Associate Elastic IP address (Associar endereço IP elástico).
4. Selecione Instance (Instância) ou Network interface (Interface de rede) e selecione o ID da instância ou da interface de rede. Selecione o endereço IP privado ao qual o endereço IP elástico será associado. Escolha Associate (Associar).

3. Dissociar um endereço IP elástico

Para alterar o recurso ao qual o endereço IP elástico está associado, primeiro é necessário desassociá-lo do recurso associado atualmente.

Para dissociar um endereço IP elástico

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Elastic IPs (IPs elásticos)
3. Selecione o endereço IP elástico e escolha Actions (Ações) e Disassociate Elastic IP address (Desassociar endereço IP elástico).
4. Quando solicitado, escolha Disassociate (Desassociar).

4. Transferir endereços IP elásticos

Esta seção descreve como transferir endereços IP elásticos de uma Conta da AWS para outra. A transferência de endereços IP elásticos pode ser útil nas seguintes situações:

- Reestruturação organizacional: use transferências de endereços IP elásticos para passar rapidamente workloads de uma Conta da AWS para outra. Nao é necessário esperar que novos endereços IP elásticos sejam listados como permitidos em seus grupos de segurança e NACLs.
- Administração de segurança centralizada: use uma conta de segurança da AWS centralizada para rastrear e transferir endereços IP elásticos que tiver a conformidade de segurança verificada.

- Recuperação de desastres: use transferências de endereços IP elásticos para remapear rapidamente IPs para workloads da Internet voltadas para o público durante eventos de emergência.

Não há cobrança pela transferência de endereços IP elásticos.

Tarefas

- Habilitar a transferência de endereços IP elásticos
- Desabilitar a transferência de endereços IP elásticos
- Aceitar um endereço IP elástico transferido

Habilitar a transferência de endereços IP elásticos

Esta seção descreve como aceitar um endereço IP elástico transferido. Observe as seguintes limitações relacionadas à habilitação de endereços IP elásticos para transferência:

- Os endereços IP elásticos podem ser transferidos de qualquer Conta da AWS (conta de origem) para qualquer outra conta da AWS na mesma região da AWS (conta de transferência).
- Ao transferir um endereço IP elástico, há um handshake de duas etapas entre as Contas da AWS. Quando a conta de origem inicia a transferência, as contas de transferência têm sete dias para aceitar a transferência do endereço IP elástico. Durante esses sete dias, a conta de origem pode visualizar a transferência pendente (por exemplo, no console da AWS ou ao usar o comando da AWS CLI describe-address-transfers). Após sete dias, a transferência expira e a propriedade do endereço IP elástico retorna à conta de origem.
- As transferências aceitas ficam visíveis para a conta de origem (por exemplo, no console da AWS ou usando o comando da AWS CLI describe-address-transfers) por 14 dias após a aceitação das transferências.
- A AWS não notifica as contas de transferência sobre solicitações pendentes de transferência de endereços IP elásticos. O proprietário da conta de origem deve notificar o proprietário da conta de transferência sobre uma solicitação de transferência de endereços IP que este deve aceitar.
- Todas as tags associadas a um endereço IP elástico que está sendo transferido são redefinidas quando a transferência é concluída.
- Não é possível transferir endereços IP elásticos alocados de grupos de endereços IPv4 públicos que você traz para sua conta da Conta da AWS (comumente chamados de grupos de endereços traga seu próprio IP (BYOIP)).

- Caso tente transferir um endereço IP elástico que tenha um registro DNS reverso associado a ele, você poderá iniciar o processo de transferência, mas a conta de transferência não poderá aceitar a transferência até que o registro DNS associado seja removido.
- Se tiver habilitado e configurado o AWS Outposts, talvez você tenha alocado endereços IP elásticos de um grupo de endereços IP pertencentes ao cliente (CoIPs). Não é possível transferir endereços IP elásticos alocados de um CoIP. No entanto, você pode usar o AWS RAM para compartilhar um CoIP com outra conta. Para obter mais informações, consulte Customer-owned IP addresses (Endereços IP pertencentes ao cliente) no Guia do usuário do AWS Outposts Outposts.
- É possível usar o Amazon VPC IPAM para rastrear a transferência de endereços IP elásticos para contas em uma organização da AWS Organizations. Para obter mais informações, consulte Visualizar histórico de endereços IP. Se um endereço IP elástico for transferido para uma Conta da AWS fora da organização, o histórico de auditoria IPAM do endereço IP elástico será perdido.

Essas etapas devem ser concluídas pela conta de origem.

Para habilitar a transferência de endereços IP elásticos

1. Verifique se você está usando a conta da AWS de origem.
2. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
3. No painel de navegação, escolha Elastic IPs (IPs elásticos)
4. Selecione um ou mais endereços IP elásticos para habilitar para transferência e escolha Actions (Ações), Enable transfer (Habilitar transferência).
5. Se você estiver transferindo vários endereços IP elásticos, verá a opção Transfer type (Tipo de transferência). Escolha uma das seguintes opções:
   - Escolha Single account (Conta única) se estiver transferindo os endereços IP elásticos para uma única conta da AWS.
   - Escolha Multiple accounts (Várias contas) se estiver transferindo os endereços IP elásticos para várias contas da AWS.
6. Em Transfer account ID (ID da conta de transferência), insira os IDs das contas da AWS para as quais deseja transferir os endereços IP elásticos.
7. Confirme a transferência inserindo **`enable`** na caixa de texto.
8. Selecione Enviar.
9. Para aceitar a transferência, consulte Aceitar um endereço IP elástico transferido. Para desabilitar a transferência, consulte Desabilitar a transferência de endereços IP elásticos.

Desabilitar a transferência de endereços IP elásticos

Esta seção descreve como desabilitar uma transferência de IP elásticos após a habilitação da transferência.

Estas etapas devem ser concluídas pela conta de origem que habilitou a transferência.

Para desabilitar uma transferência de endereço IP elástico

1. Verifique se você está usando a conta da AWS de origem.
2. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
3. No painel de navegação, escolha Elastic IPs (IPs elásticos)
4. Na lista de recursos de IPs elásticos, verifique se a propriedade que mostra o status de transferência da coluna está habilitada.
5. Selecione um ou mais endereços IP elásticos que tenham Transfer status (Status de transferência) Pending (Pendente) e escolha Actions (Ações), Disable transfer (Desabilitar transferência).
6. Confirme digitando **`disable`** na caixa de texto.
7. Selecione Enviar.

Aceitar um endereço IP elástico transferido

Esta seção descreve como aceitar um endereço IP elástico transferido.

Ao transferir um endereço IP elástico, há um handshake de duas etapas entre as Contas da AWS. Quando a conta de origem inicia a transferência, as contas de transferência têm sete dias para aceitar a transferência do endereço IP elástico. Durante esses sete dias, a conta de origem pode visualizar a transferência pendente (por exemplo, no console da AWS ou ao usar o comando da AWS CLI describe-address-transfers). Após sete dias, a transferência expira e a propriedade do endereço IP elástico retorna à conta de origem.

Ao aceitar transferências, observe as seguintes exceções que podem ocorrer e como resolvê-las:

- AddressLimitExceeded: se sua conta de transferência tiver excedido a cota de endereços IP elásticos, a conta de origem poderá habilitar a transferência de endereços IP elásticos, mas essa exceção ocorrerá quando a conta de transferência tentar aceitar a transferência. Por padrão, todas as contas da AWS estão limitadas a 5 endereços IP elásticos por região. Consulte Limite

de endereços IP elásticos no Guia do usuário do Amazon EC2 para obter instruções sobre como aumentar o limite.

- InvalidTransfer.AddressCustomPtrSet: se você ou alguém da sua organização tiver configurado o endereço IP elástico que você está tentando transferir para usar pesquisa reversa de DNS, a conta de origem poderá habilitar a transferência para o endereço IP elástico, mas essa exceção ocorrerá quando a conta de transferência tentar aceitar a transferência. Para resolver esse problema, a conta de origem deverá remover o registro de DNS do endereço IP elástico. Para obter mais informações, consulte Remover um registro de DNS reverso no Guia do usuário do Amazon EC2.
- InvalidTransfer.AddressAssociated: se houver um endereço IP elástico associado a uma instância do ENI ou EC2, a conta de origem poderá habilitar a transferência para o endereço IP elástico, mas essa exceção ocorrerá quando a conta de transferência tentar aceitar a transferência. Para resolver esse problema, a conta de origem deve desassociar o endereço IP elástico. Para obter mais informações, consulte Dissociar um endereço IP elástico no Guia do usuário do Amazon EC2.

Para quaisquer outras exceções, entre em contato com o Support.

Essas etapas devem ser concluídas pela conta de transferência.

Para aceitar uma transferência de endereço IP elástico

1. Verifique se você está usando a conta de transferência.
2. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
3. No painel de navegação, escolha Elastic IPs (IPs elásticos)
4. Escolha Actions (Ações), Accept transfer (Aceitar transferência).
5. Quando a transferência for aceita, nenhuma tag associada ao endereço IP elástico que está sendo transferido será transferida com o endereço IP elástico. Se desejar definir uma etiqueta Name (Nome) para o endereço IP elástico que está aceitando, selecione Create a tag with a key of 'Name' and a value that you specify (Criar uma tag com uma chave “Nome” e um valor especificado por você).
6. Insira o endereço IP elástico que deseja transferir.
7. Se você estiver aceitando vários endereços IP elásticos transferidos, escolha Add address (Adicionar endereço) para inserir um endereço IP elástico adicional.
8. Selecione Enviar.

5. Liberar um endereço IP elástico

Se não for mais necessário um endereço IP elástico, recomendamos liberá-lo. Você será cobrado por qualquer endereço IP elástico que for alocado para uso com uma VPC mesmo que ele não seja associado a uma instância. O endereço IP elástico não deve ser associado a uma instância ou interface de rede.

Para liberar um endereço IP elástico

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Elastic IPs (IPs elásticos)
3. Selecione o endereço IP elástico e escolha Actions (Ações), Release Elastic IP addresses (Liberar endereços IP elásticos).
4. Quando solicitado, escolha Release.

6. Recuperar um endereço IP elástico

Se você liberar um endereço IP elástico e mudar de ideia, talvez seja possível recuperá-lo. Não será possível recuperar o endereço IP elástico se ele tiver sido alocado a outra conta da AWS, ou se isso resultar em endereços IP elásticos acima da sua cota.

É possível recuperar um endereço IP elástico usando a API do Amazon EC2 ou uma ferramenta de linha de comando.

Para recuperar um endereço IP elástico usando a AWS CLI

Use o comando allocate-address e especifique o endereço IP usando o parâmetro `--address`.

```
aws ec2 allocate-address --domain vpc --address 203.0.113.3
```

Visão geral da linha de comando

É possível executar as tarefas descritas neste tópico usando a linha de comando ou uma API. Para obter mais informações sobre as interfaces de linha de comando e sobre a lista de ações de API disponíveis, consulte Trabalhar com a Amazon VPC.

Aceitar uma transferência de endereço IP elástico

- accept-address-transfer (AWS CLI)

- Approve-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Alocar um endereço IP elástico

- allocate-address (AWS CLI)
- New-EC2Address (AWS Tools for Windows PowerShell)

Associar um endereço IP elástico a uma instância ou interface de rede

- associate-address (AWS CLI)
- Register-EC2Address (AWS Tools for Windows PowerShell)

Descrever transferências de endereços IP elásticos

- describe-address-transfers (AWS CLI)
- Get-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Desabilitar a transferência de endereços IP elásticos

- disable-address-transfer (AWS CLI)
- Disable-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Dissociar um endereço IP elástico

- disassociate-address (AWS CLI)
- Unregister-EC2Address (AWS Tools for Windows PowerShell)

Habilitar a transferência de endereços IP elásticos

- enable-address-transfer (AWS CLI)
- Enable-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Liberar um endereço IP elástico

- release-address (AWS CLI)

- Remove-EC2Address (AWS Tools for Windows PowerShell)

Aplicar uma tag em um endereço IP elástico

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)

Visualizar endereços IP elásticos

- describe-addresses (AWS CLI)
- Get-EC2Address (AWS Tools for Windows PowerShell)

Conectar sua VPC a outras VPCs e redes usando um gateway de trânsito

Você pode conectar suas nuvens virtuais privadas (VPC) e redes on-premises usando um gateway de trânsito, que atua como um hub central, encaminhando o tráfego entre VPCs, conexões VPN e conexões do AWS Direct Connect.

Um dos principais benefícios do uso de um gateway de trânsito é a capacidade de centralizar e simplificar o gerenciamento da conectividade entre suas VPCs e redes on-premises. Em vez de configurar várias conexões de VPN ou links Direct Connect, é possível utilizar o gateway de trânsito como um único ponto de integração, o que pode ajudar a reduzir a complexidade geral e a sobrecarga operacional da arquitetura de rede.

O preço do uso de um gateway de trânsito é baseado no volume de dados transferidos pelo gateway. Há uma taxa por GB para dados transferidos para dentro e para fora do gateway de trânsito, bem como uma taxa separada por hora para o próprio recurso do gateway de trânsito. O preço específico pode variar de acordo com a região da AWS e está sujeito a alterações. Por isso, é importante consultar a página de preços atual do AWS Transit Gateway para obter as informações mais atualizadas. Ao entender o modelo de preços dos gateways de trânsito, é possível planejar e orçar melhor os custos contínuos associados a esse serviço de rede da AWS. Isso, combinado com as eficiências operacionais e os benefícios de conectividade, torna os gateways de trânsito uma opção atraente para organizações que buscam criar soluções de nuvem híbrida escaláveis e econômicas.

A tabela apresentada a seguir descreve alguns casos de uso comuns para gateways de trânsito. Para obter mais informações sobre cada caso de uso, consulte Example transit gateway scenarios no Guia do usuário do AWS Transit Gateway.

Exemplo	Uso
Roteador centralizado	Configure seu Transit Gateway como roteador centralizado que conecta todas as suas conexões de VPCs, AWS Direct Connect e AWS Site-to-Site VPN.
VPCs isoladas	Configure o Transit Gateway como vários roteadores isolados. É semelhante ao uso de vários gateways de trânsito, mas permite mais flexibilidade nos casos em que as rotas e os anexos puderem mudar.
VPCs isoladas com serviços compartilhados	É possível configurar seu Transit Gateway como vários roteadores isolados que usam um serviço compartilhado. É semelhante ao uso de vários gateways de trânsito, mas permite mais flexibilidade nos casos em que as rotas e os anexos puderem mudar.

Para obter mais informações, consulte AWS Transit Gateway.

Conectar sua VPC a redes remotas usando a AWS Virtual Private Network

É possível conectar sua VPC a redes e usuários remotos usando as opções de conectividade por VPN a seguir.

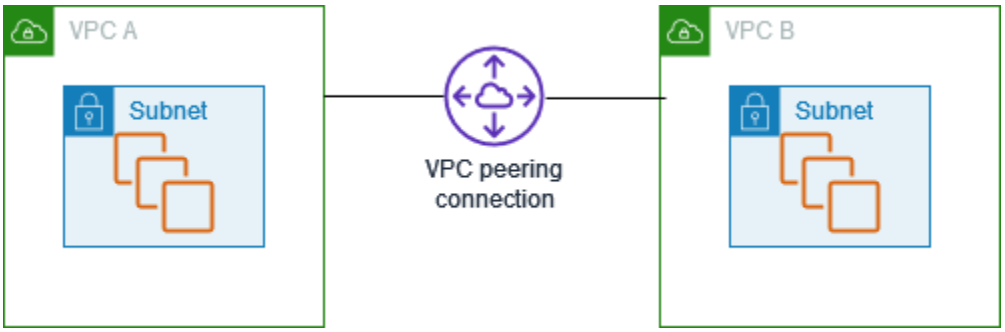
Opção de conexão VPN	Descrição
AWS Site-to-Site VPN	Crie uma conexão VPN de IPsec entre sua VPC e sua rede remota. No lado da AWS da conexão da Site-to-Site VPN, um gateway privado virtual ou um gateway de trânsito fornece dois endpoints de VPN (túneis) para fins de failover automático. Configure seu dispositivo de

Opção de conexão VPN	Descrição
	gateway do cliente no lado remoto da conexão da Site-to-Site VPN. Para obter mais informações, consulte o Manual do usuário do AWS Site-to-Site VPN.
AWS Client VPN	O AWS Client VPN é um serviço de VPN baseado no cliente que protege o acesso aos recursos da AWS ou a sua rede on-premises. Com o AWS Client VPN, é possível configurar um endpoint para garantir a segurança da conexão de clientes por meio de uma sessão de VPN com TLS. Isso permite que os clientes acessem na AWS ou on-premis es de qualquer lugar usando um cliente de VPN baseado em OpenVPN. Para obter mais informações, consulte o Guia do administrador do AWS Client VPN.
AWS VPN CloudHub	Se tiver mais de uma rede remota (por exemplo, várias filiais), você poderá criar várias conexões do AWS Site-to-Site VPN por meio do gateway privado virtual, permitindo a comunicação entre as redes. Para obter mais informações, consulte Garantia de comunicação segura entre sites usando o VPN CloudHub no Manual do usuário do AWS Site-to-Site VPN.
Dispositivo VPN de software terceirizado	Você pode criar uma conexão VPN para sua rede remota usando uma instância do Amazon EC2 na VPC que está executando um dispositi vo de VPN de software de terceiros. A AWS não fornece nem mantém dispositivos de VPN de software de terceiros, mas é possível escolher uma opção entre os diversos produtos fornecidos por parceiros e comunidades de código aberto. Encontre dispositivos VPN de software de terceiros no AWS Marketplace.

Você também pode usar AWS Direct Connect para criar uma conexão privada de uma rede remota para a VPC. Combine essa conexão com o AWS Site-to-Site VPN para criar uma conexão criptografada IPsec. Para obter mais informações, consulte O que é o AWS Direct Connect? no Manual do usuário do AWS Direct Connect.

Conectar VPCs usando emparelhamento da VPC

Uma conexão de emparelhamento de VPC é um recurso de rede que permite a comunicação direta e segura entre duas nuvens privadas virtuais (VPCs) dentro da infraestrutura da AWS. Essa conexão privada permite que os recursos nas VPCs emparelhadas interajam entre si como se fossem parte da mesma rede, eliminando a necessidade de atravessar a Internet pública.



O processo de criação de uma conexão de emparelhamento de VPC aproveita a infraestrutura de VPC existente para estabelecer essa conexão sem a necessidade de um gateway, do AWS Site-to-Site VPN ou de qualquer hardware físico adicional. Esse design garante que não haja um único ponto de falha ou gargalo na largura de banda.

Uma das principais vantagens de uma conexão de emparelhamento de VPC é a capacidade de conectar VPCs em diferentes contas da AWS ou até mesmo em diferentes regiões da AWS. Essa flexibilidade permite que as organizações integrem perfeitamente seus recursos de nuvem, estejam eles na mesma conta ou espalhados por várias contas e localizações geográficas. A natureza privada da conexão também garante que todo o tráfego de dados entre as VPCs emparelhadas permaneça dentro da rede da AWS, sem nunca atravessar a Internet pública.

Os casos de uso para conexões de emparelhamento de VPC são abrangentes. As organizações podem utilizar esse recurso para permitir a comunicação segura entre diferentes camadas de uma aplicação (como servidores Web e servidores de banco de dados), facilitar o compartilhamento de recursos entre várias equipes ou unidades de negócios ou até mesmo habilitar arquiteturas de nuvem híbrida conectando redes on-premises às suas AWS VPCs.

Uma conexão de emparelhamento da VPC é uma conexão de redes entre duas VPCs que permite rotear o tráfego entre elas de forma privada. Recursos em VPC emparelhadas podem se comunicar uns com os outros como se estivessem na mesma rede. É possível criar uma conexão de emparelhamento da VPC entre suas próprias VPCs, com uma VPC em outra Conta da AWS ou com uma VPC em uma região diferente da AWS. O tráfego entre VPCs emparelhadas nunca passa pela Internet pública.

Para obter mais informações, consulte o Amazon VPC Peering Guide (Guia de emparelhamento da Amazon VPC).

Monitoramento da sua VPC

Você pode usar as seguintes ferramentas para monitorar o tráfego ou o acesso à rede em sua nuvem privada virtual (VPC).

Logs de fluxo da VPC

Você pode usar o VPC Flow Logs para capturar informações detalhadas sobre o tráfego que chega e sai das interfaces de rede em suas VPCs.

Amazon CloudWatch Internet Monitor

Você pode usar o monitor de internet para ter visibilidade de como os problemas de internet afetam a performance e a disponibilidade entre as aplicações hospedadas na AWS e os usuários finais. Você também pode explorar, quase em tempo real, como aprimorar a latência prevista da aplicação alternando para o uso de outros serviços ou redirecionando o tráfego para a workload por diferentes Regiões da AWS. Para obter mais informações, consulte a Uso do monitor de internet do Amazon CloudWatch.

IP Address Manager (IPAM) da Amazon VPC

Você pode usar o IPAM para planejar, rastrear e monitorar endereços IP de suas workloads. Para mais informações, consulte IP Address Manager (Gerenciador de endereço IP).

Espelhamento de tráfego

É possível usar esse recurso para copiar o tráfego de rede de uma interface de rede de uma instância do Amazon EC2 e enviá-lo para dispositivos de segurança e monitoramento fora de banda para inspeção detalhada de pacotes. Você pode detectar anomalias de rede e segurança, obter insights operacionais, implementar controles de conformidade e segurança, e solucionar problemas. Para mais informações, consulte Traffic Mirroring (Espelhamento de tráfego).

Reachability Analyzer

Você pode usar essa ferramenta para analisar e depurar a acessibilidade da rede entre dois recursos em sua VPC. Após especificar os recursos de origem e de destino, o Reachability Analyzer produz detalhes de salto a salto do caminho virtual entre eles quando eles são alcançáveis e identifica o componente bloqueador quando eles estão inacessíveis. Para obter mais informações, consulte Analisador de Acessibilidade.

Network Access Analyzer

Você pode usar o Network Access Analyzer para entender o acesso de rede aos seus recursos. Isso ajuda você a identificar melhorias no procedimento de segurança da rede e demonstrar que sua rede atende a requisitos específicos de conformidade. Para mais informações, consulte Network Access Analyzer.

Logs do CloudTrail

Você pode usar o AWS CloudTrail para capturar informações detalhadas sobre as chamadas feitas para a API da Amazon VPC. Você pode usar os logs gerados pelo CloudTrail para determinar quais chamadas foram feitas, o endereço IP de origem da chamada, quem fez a chamada, quando ela foi feita etc. Para obter mais informações, consulte Registro em log das chamadas de API do Amazon EC2 usando o AWS CloudTrail no Guia do usuário do Amazon EC2.

Como registrar tráfego IP em log com logs de fluxo da VPC

O VPC Flow Logs é um recurso que possibilita que você capture informações sobre o tráfego de IP para e proveniente de interfaces de rede da VPC. Os dados do log de fluxo podem ser publicados nos seguintes locais: Amazon CloudWatch Logs, Amazon S3 ou Amazon Data Firehose. O caminho de entrega configurado e as permissões que permitem que os logs de tráfego de rede sejam enviados para um destino como o CloudWatch Logs ou o S3 são chamados de assinaturas. Depois de criar um log de fluxo, você poderá recuperar e visualizar os registros do log de fluxo no grupo de logs, no bucket ou no fluxo de entrega configurado.

Os logs de fluxo podem ajudar em diversas tarefas, como:

- Diagnosticar regras de grupo de segurança excessivamente restritivas
- Monitorar o tráfego que chega à sua instância
- Determinar a direção de entrada e saída do tráfego das interfaces de rede

Os dados do log de fluxo são coletados fora do caminho do tráfego de rede e, portanto, não afetam o throughput nem a latência da rede. É possível criar ou excluir logs de fluxo sem qualquer risco de impacto na performance da rede.

> **Note**
>
> Esta seção trata apenas dos logs de fluxo para VPCs. Para obter informações sobre os logs de fluxo para gateways de trânsito lançados na versão 6, consulte Logging network traffic using Transit Gateway Flow Logs no Guia do usuário do Amazon VPC Transit Gateways.

Conteúdo

Noções básicas de logs de fluxo

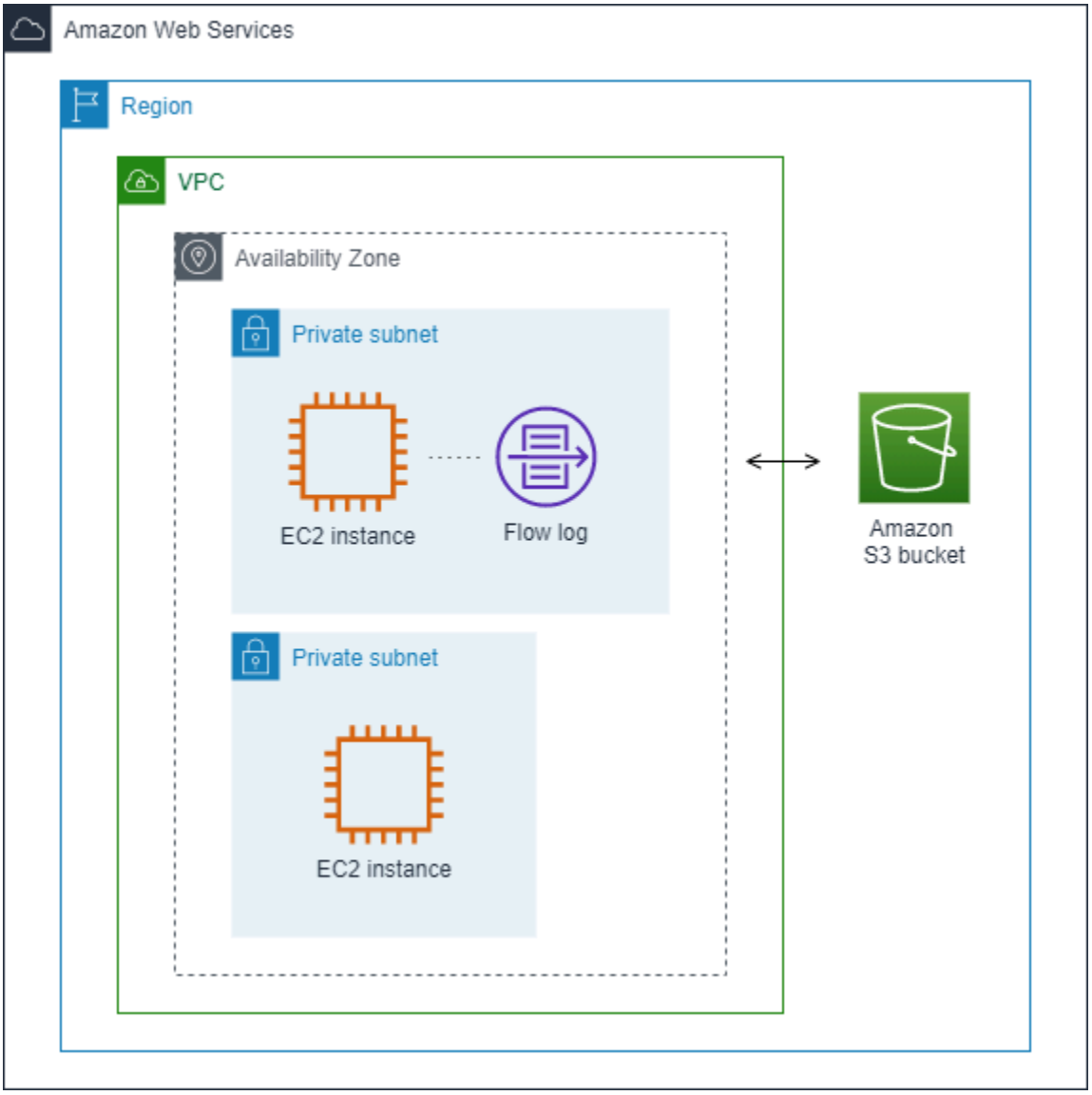
É possível criar um log de fluxo para VPC, sub-rede ou interface de rede. Se você criar um log de fluxo para uma sub-rede ou VPC, toda interface de rede na sub-rede ou VPC será monitorada.

Os dados de log de fluxo para uma interface de rede monitorada são registrados como registros de log de fluxo, que são eventos de log que consistem em campos que descrevem o fluxo de tráfego. Para obter mais informações, consulte Registros de log de fluxo.

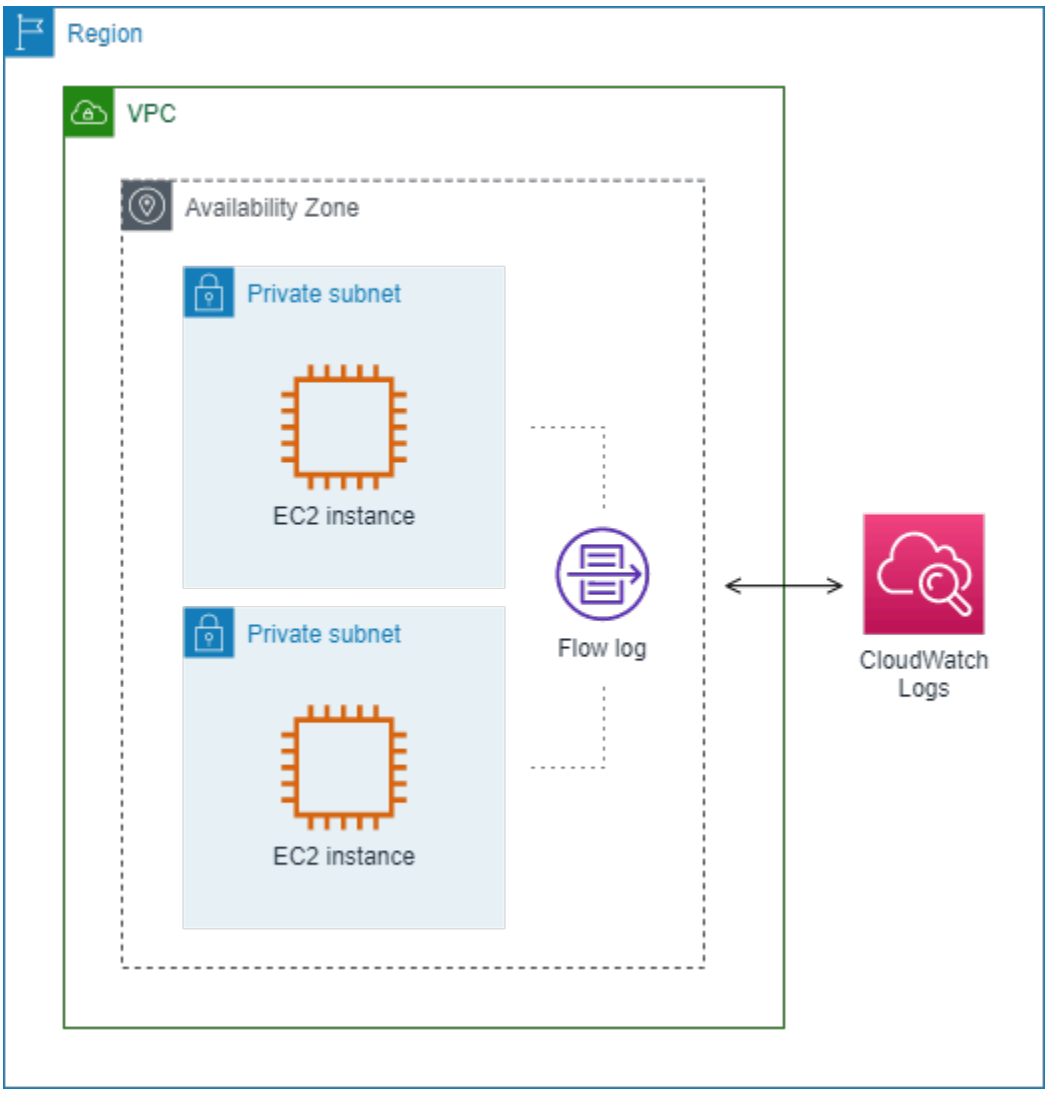
Para criar um log de fluxo, especifique:

- O recurso para o qual criar o log de fluxo
- O tipo de tráfego a ser capturado (tráfego aceito, tráfego rejeitado ou todo o tráfego)
- Os destinos em que você quer publicar os dados de log de fluxo

No exemplo a seguir, crie um log de fluxo que capture o tráfego aceito para a interface de rede de uma das instâncias do EC2 em uma sub-rede privada e publica os registros de log de fluxo em um bucket do Amazon S3.



No seguinte exemplo, um log de fluxo captura todo o tráfego para a sub-rede e publica os registros do log de fluxo no Amazon CloudWatch Logs. O log de fluxo captura o tráfego para todas as interfaces de rede na sub-rede.



Depois que você criar um log de fluxo, pode demorar alguns minutos para começar a coletar e publicar dados nos destinos selecionados. Os logs de fluxo não capturam streams de logs em tempo real para suas interfaces de rede. Para ter mais informações, consulte 2. Criar um log de fluxo.

Se você iniciar uma instância na sua sub-rede depois de criar um log de fluxo para a sua sub-rede ou VPC, criaremos um fluxo de logs (para o CloudWatch Logs) ou objeto de arquivo de log (para o Amazon S3) para a nova interface de rede assim que houver tráfego de rede para a interface de rede.

Você pode criar logs de fluxo para interfaces de rede que são criadas por outros serviços da AWS, como:

- Elastic Load Balancing
- Amazon RDS

- Amazon ElastiCache
- Amazon Redshift
- Amazon WorkSpaces
- Gateways NAT
- Gateways de trânsito

Independentemente do tipo de interface de rede, é necessário usar o console ou a API do Amazon EC2 para criar um log de fluxo para uma interface de rede.

É possível aplicar tags aos logs de fluxo. Cada tag consiste de uma chave e um valor opcional, que podem ser definidos. As tags podem ajudar você a organizar seus logs de fluxo. Por exemplo, por finalidade ou proprietário.

Caso não precise mais de um log de fluxo, é possível excluí-lo. A exclusão de um log de fluxo desabilita o serviço de log de fluxo para o recurso, de modo que novos registros de log de fluxo não são criados nem publicados. A exclusão de um log de fluxo não exclui qualquer dado existente do log de fluxo. Depois de excluir um log de fluxo, você pode excluir os dados do log de fluxo diretamente do destino quando terminar de usá-lo. Para ter mais informações, consulte 4. Excluir um log de fluxo.

Registros de log de fluxo

Um registro de log de fluxo representa um fluxo de rede na VPC. Por padrão, cada registro captura um fluxo de tráfego de protocolo de Internet (IP) da rede (caracterizado por 5 tuplas em uma base de interface de rede) que ocorre dentro de um intervalo de agregação, também referido como uma janela de captura.

Cada registro é uma string com campos separados por espaços. Um registro inclui valores para os diferentes componentes do fluxo IP como, por exemplo, a origem, o destino e o protocolo.

Ao criar um log de fluxo, é possível usar o formato padrão do registro de log de fluxo ou especificar um formato personalizado.

Tópicos

- Campos disponíveis

Intervalo de agregação

O intervalo de agregação é o período durante o qual um fluxo específico é capturado e agregado em um registro de log de fluxo. Por padrão, o intervalo de agregação máximo é de dez minutos. Ao criar um log de fluxo, você pode especificar um intervalo de agregação máximo de 1 minuto, opcionalmente. Os logs de fluxo com um intervalo de agregação máximo de 1 minuto geram um volume mais alto de registros de log de fluxo que os logs de fluxo com um intervalo de agregação máximo de 10 minutos.

Quando uma interface de rede é anexada a uma instância baseada em Nitro, o intervalo de agregação é sempre 1 minuto ou menos, independentemente do intervalo de agregação máximo especificado.

Depois que os dados forem capturados em um intervalo de agregação, será necessário tempo adicional para processar e publicar os dados no CloudWatch Logs e no Amazon S3. O serviço de log de fluxo geralmente fornece logs para o CloudWatch Logs em cerca de 5 minutos e para o Amazon S3 em cerca de 10 minutos. No entanto, a entrega de logs baseia-se no melhor esforço, e seus registros podem ser atrasados além do tempo de entrega típico.

Formato padrão

Com o formato padrão, os registros de log de fluxo incluem os campos da versão 2, na ordem mostrada na tabela de campos disponíveis. Não é possível personalizar ou alterar o formato padrão. Para capturar campos adicionais disponíveis ou um subconjunto de campos diferente, especifique um formato personalizado em vez disso.

Formato personalizado

Com um formato personalizado, você especifica quais campos estão incluídos nos registros de log de fluxo e em qual ordem. Isso permite que você crie logs de fluxo específicos para suas necessidades e omita campos que não são relevantes. Usar um formato personalizado pode diminuir a necessidade de processos separados para extrair informações específicas dos logs de fluxo publicados. É possível especificar qualquer quantidade de campos disponíveis do log de fluxo, mas deve-se especificar pelo menos um.

Campos disponíveis

A tabela a seguir descreve todos os campos disponíveis para um registro de log de fluxo. A coluna Versão indica a versão do VPC Flow Logs na qual o campo foi introduzido. O formato padrão inclui todos os campos da versão 2, na mesma ordem em que aparecem na tabela.

Ao publicar dados de log de fluxo no Amazon S3, o tipo de dados para os campos dependerá do formato do log de fluxo. Se o formato estiver como texto sem formatação, todos os campos serão do tipo STRING. Se o formato for Parquet, consulte a tabela para os tipos de dados de campo.

Se um campo não for aplicável ou não puder ser computado para um registro específico, o registro exibirá o símbolo '-' para essa entrada. Os campos de metadados que não vêm diretamente do cabeçalho do pacote são aproximações e seus valores podem estar ausentes ou imprecisos.

Campo	Descrição	Versão
version	A versão dos logs de fluxo da VPC. Se você usar o formato padrão, a versão será 2. Se você usar um formato personalizado, a versão será a versão mais alta entre os campos especificados. Por exemplo, se você especificar apenas os campos da versão 2, a versão será 2. Se você especificar uma mistura de campos das versões 2, 3 e 4, a versão será 4. Tipo de dados em Parquet: INT_32	2
account-id	O ID da conta da AWS do proprietário da interface de rede de origem para a qual o tráfego é registrado. Se a interface de rede for criada por um serviço da AWS, por exemplo, ao criar um endpoint da VPC ou Network Load Balancer, o registro poderá exibir unknown para esse campo. Tipo de dados em Parquet: STRING	2
interface-id	O ID da interface de rede para a qual o tráfego é registrado. Tipo de dados em Parquet: STRING	2
srcaddr	No caso do tráfego de entrada, este é o endereço IP da origem do tráfego. No caso do tráfego de saída, este é o endereço IPv4	2

Campo	Descrição	Versão
	privado ou o endereço IPv6 da interface de rede que envia o tráfego. Consulte também pkt-srcaddr. Tipo de dados em Parquet: STRING	
dstaddr	O endereço de destino do tráfego de saída ou o endereço IPv4 ou IPv6 da interface de rede do tráfego de entrada na interface de rede. O endereço IPv4 da interface de rede sempre é o respectivo endereço IPv4 privado. Consulte também pkt-dstaddr. Tipo de dados em Parquet: STRING	2
srcport	A porta de origem do tráfego. Tipo de dados em Parquet: INT_32	2
dstport	A porta de destino do tráfego. Tipo de dados em Parquet: INT_32	2
protocol	O número do protocolo IANA do tráfego. Para obter mais informaçõ es, consulte Números de Protocolo da Internet Designados. Tipo de dados em Parquet: INT_32	2
packets	O número de pacotes transferidos durante o fluxo. Tipo de dados em Parquet: INT_64	2
bytes	O número de bytes transferidos durante o fluxo. Tipo de dados em Parquet: INT_64	2
start	O tempo, em segundos Unix, quando o primeiro pacote de fluxo foi recebido no intervalo de agregação. Isso pode ocorrer até 60 segundos após o pacote ter sido transmitido ou recebido na interface de rede Tipo de dados em Parquet: INT_64	2

Campo	Descrição	Versão
end	O tempo, em segundos Unix, quando o último pacote de fluxo foi recebido dentro do intervalo de agregação. Isso pode ocorrer até 60 segundos após o pacote ter sido transmitido ou recebido na interface de rede Tipo de dados em Parquet: INT_64	2
action	A ação associada ao tráfego: • ACCEPT: o tráfego foi aceito. • REJECT: o tráfego foi rejeitado. Por exemplo, o tráfego não foi permitido pelos grupos de segurança ou ACLs de rede, ou os pacotes chegaram depois que a conexão foi fechada. Tipo de dados em Parquet: STRING	2

Campo	Descrição	Versão
log-status	O status de registro do log de fluxo: • OK: os dados são registrados em log normalmente nos destinos selecionados. • NODATA: não havia nenhum tráfego de rede para ou proveniente da interface de rede durante o intervalo de agregação. • SKIPDATA: alguns registros de log de fluxo foram ignorados durante o intervalo de agregação. Isso pode ocorrer em virtude de uma restrição de capacidade interna ou de um erro interno. Alguns registros de log de fluxo podem ser ignorados durante o intervalo de agregação (consulte log-status em Campos disponíveis). Isso pode ocorrer em virtude de uma restrição de capacidade interna da AWS ou de um erro interno. Se você estiver usando o AWS Cost Explorer para visualizar as cobranças dos logs de fluxo da VPC e alguns logs de fluxo forem ignorados durante o intervalo de agregação de logs de fluxo, o número de logs de fluxo relatados AWS Cost Explorer será maior do que o número de logs de fluxo publicados pela Amazon VPC. Tipo de dados em Parquet: STRING	2
vpc-id	O ID da VPC que contém a interface de rede para a qual o tráfego é registrado. Tipo de dados em Parquet: STRING	3
subnet-id	O ID da sub-rede que contém a interface de rede para a qual o tráfego é registrado. Tipo de dados em Parquet: STRING	3

Campo	Descrição	Versão
instance-id	O ID da instância associada à interface de rede para a qual o tráfego é registrado, caso a instância seja de sua propriedade. Retorna um símbolo “-” para uma interface de rede gerenciada pelo solicitante; por exemplo, a interface de rede de um gateway NAT. Tipo de dados em Parquet: STRING	3

Campo	Descrição	Versão
tcp-flags	O valor da máscara de bits para os seguintes sinalizadores TCP: • FIN: 1 • SYN: 2 • RST: 4 • SYN-ACK: 18 Se nenhum sinalizador compatível for registrado, o valor do sinalizador TCP será 0. Por exemplo, no caso de sinalizadores como ACK ou PSH, que não são suportados pelo registro de tcp-flags, o resultado para registros de tráfego contendo esses sinalizadores não suportados será 0 para tcp-flags. Entretant o, se um sinalizador não suportado estiver acompanhado por um sinalizador suportado, o valor do sinalizador suportado será informado. Por exemplo, se o ACK fizer parte do SYN-ACK, o relatório indicará o valor 18. Se houver um registro como SYN +ECE, onde SYN é um sinalizador suportado e ECE não é, o valor do sinalizador TCP será 2. O valor “-” será atribuído para casos nos quais a combinação de sinalizadores seja inválida e não seja possível calcular o valor. Se nenhum sinalizador for enviado, o valor do sinalizador TCP será 0. Os sinalizadores TCP podem ser processados com o operador OR durante o intervalo de agregação. Para conexões curtas, os sinalizadores podem ser definidos na mesma linha no registro de log de fluxo, por exemplo, 19 para SYN-ACK e FIN, e 3 para SYN e FIN. Para ver um exemplo, consulte Sequência de sinalizadores TCP. Para obter informações gerais sobre sinalizadores TCP (por exemplo, o significado de sinalizadores FIN, SYN e ACK), consulte Estrutura de segmentos TCP, na Wikipédia. Tipo de dados em Parquet: INT_32	3

Campo	Descrição	Versão
type	O tipo de tráfego. Os valores possíveis são: IPv4 | IPv6 | EFA. Para obter mais informações, consulte Elastic Fabric Adapter. Tipo de dados em Parquet: STRING	3
pkt-srcaddr	O endereço IP de origem (original) no nível do pacote do tráfego. Use esse campo com o campo srcaddr para diferenciar o endereço IP de uma camada intermediária pela qual o tráfego flui e o endereço IP de origem original do tráfego. Por exemplo, quando o tráfego flui por uma interface de rede para um gateway NAT ou quando o endereço IP de um pod no Amazon EKS é diferente do endereço IP da interface de rede do nó da instância em que o dispositivo está em execução (para comunicação dentro de uma VPC). Tipo de dados em Parquet: STRING	3
pkt-dstaddr	O endereço IP de destino (original) no nível do pacote do tráfego. Use esse campo com o campo dstaddr para diferenciar o endereço IP de uma camada intermediária pela qual o tráfego flui e o endereço IP de destino final do tráfego. Por exemplo, quando o tráfego flui por uma interface de rede para um gateway NAT ou quando o endereço IP de um pod no Amazon EKS é diferente do endereço IP da interface de rede do nó da instância em que o dispositivo está em execução (para comunicação dentro de uma VPC). Tipo de dados em Parquet: STRING	3
region	A região que contém a interface de rede para a qual o tráfego é registrado. Tipo de dados em Parquet: STRING	4

Campo	Descrição	Versão
az-id	O ID da zona de disponibilidade que contém a interface de rede para a qual o tráfego é registrado. Se o tráfego for de uma sublocalização, o registro exibirá um símbolo '-' para este campo. Tipo de dados em Parquet: STRING	4
sublocation-type	O tipo de sublocalização que é retornado no campo sublocation-id. Os valores possíveis são: wavelength | outpost | localzone . Se o tráfego não for de uma sublocalização, o registro exibirá um símbolo '-' para este campo. Tipo de dados em Parquet: STRING	4
sublocation-id	O ID da sublocalização que contém a interface de rede para a qual o tráfego é registrado. Se o tráfego não for de uma sublocalização, o registro exibirá um símbolo '-' para este campo. Tipo de dados em Parquet: STRING	4
pkt-src-aws-service	O nome do subconjunto de intervalos de endereços IP para o campo pkt-srcaddr, se o endereço IP de origem for para um serviço da AWS. Se o pkt-srcaddr pertencer a um intervalo sobreposto, pkt-src-aws-service mostrará apenas um dos códigos de serviço da AWS. Os valores possíveis são: AMAZON | AMAZON_APPFLOW | AMAZON_CONNECT | API_GATEWAY | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR | KINESIS_VIDEO_STREAMS | ROUTE53 | ROUTE53_HEALTHCHECKS | ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_RESOLVER | S3 | WORKSPACES_GATEWAYS. Tipo de dados em Parquet: STRING	5

Campo	Descrição	Versão
pkt-dst-aws-service	O nome do subconjunto de intervalos de endereços IP para o campo pkt-dstaddr, se o endereço IP de destino for para um serviço da AWS. Para uma lista de valores possíveis, consulte o campo pkt-src-aws-service. Tipo de dados em Parquet: STRING	5
flow-direction	O sentido do fluxo em relação à interface onde o tráfego é capturado. Os valores possíveis são: ingress | egress. Tipo de dados em Parquet: STRING	5
traffic-path	O trajeto que o tráfego de saída leva ao destino. Para determinar se o tráfego é de saída, verifique o campo flow-direction. Os valores possíveis são conforme o seguintes. Se nenhum dos valores se aplicar, o campo será definido como -. • 1: por meio de outro recurso na mesma VPC, incluindo recursos que criam uma interface de rede na VPC • 2: por meio de um gateway da internet ou de um VPC endpoint de gateway • 3: por meio de um gateway privado virtual • 4: por meio de uma conexão de emparelhamento de VPC dentro da região • 5: por meio de uma conexão de emparelhamento de VPC entre regiões • 6: por meio de um gateway local • 7: por meio de um endpoint da VPC de gateway (somente instâncias baseadas em Nitro) • 8: por meio de um gateway da Internet (somente instâncias baseadas em Nitro) Tipo de dados em Parquet: INT_32	5

Campo	Descrição	Versão
ecs-cluster-arn	Nome do recurso da AWS (ARN) do cluster do ECS se o tráfego for proveniente de uma tarefa do ECS em execução. Para incluir esse campo na sua assinatura, você vai precisar de permissão para chamar ecs:ListClusters. Tipo de dados em Parquet: STRING	7
ecs-cluster-name	Nome do cluster do ECS se o tráfego for proveniente de uma tarefa do ECS em execução. Para incluir esse campo na sua assinatura, você vai precisar de permissão para chamar ecs:ListClusters. Tipo de dados em Parquet: STRING	7
ecs-container-instance-arn	ARN da instância de contêiner do ECS se o tráfego for proveniente de uma tarefa do ECS em execução em uma instância do EC2. Se o provedor de capacidade for AWS Fargate, esse campo será “-”. Para incluir esse campo na sua assinatura, você vai precisar de permissão para chamar ecs:ListClusters e ecs:ListContainerInstances. Tipo de dados em Parquet: STRING	7
ecs-container-instance-id	ID da instância de contêiner do ECS se o tráfego for proveniente de uma tarefa do ECS em execução em uma instância do EC2. Se o provedor de capacidade for AWS Fargate, esse campo será “-”. Para incluir esse campo na sua assinatura, você vai precisar de permissão para chamar ecs:ListClusters e ecs:ListContainerInstances. Tipo de dados em Parquet: STRING	7
ecs-container-id	ID de runtime do Docker do contêiner se o tráfego for de uma tarefa do ECS em execução. Se houver um ou mais contêineres na tarefa do ECS, esse será o ID de runtime do Docker do primeiro contêiner. Para incluir esse campo na sua assinatura, você vai precisar de permissão para chamar ecs:ListClusters. Tipo de dados em Parquet: STRING	7

Campo	Descrição	Versão
ecs-second-container-id	ID de runtime do Docker do contêiner se o tráfego for de uma tarefa do ECS em execução. Se houver mais de um contêiner na tarefa do ECS, esse será o ID de runtime do Docker do segundo contêiner . Para incluir esse campo na sua assinatura, você vai precisar de permissão para chamar ecs:ListClusters. Tipo de dados em Parquet: STRING	7
ecs-service-name	Nome do serviço do ECS se o tráfego for proveniente de uma tarefa do ECS em execução e a tarefa do ECS for iniciada por um serviço do ECS. Se a tarefa do ECS não for iniciada por um serviço do ECS, esse campo será “-”. Para incluir esse campo na sua assinatura, você vai precisar de permissão para chamar ecs:ListClusters e ecs:ListServices. Tipo de dados em Parquet: STRING	7
ecs-task-definition-arn	O ARN da definição da tarefa do ECS se o tráfego for proveniente de uma tarefa do ECS em execução. Para incluir esse campo na sua assinatura, você vai precisar de permissão para chamar ecs:ListClusters e ecs:ListTaskDefinitions. Tipo de dados em Parquet: STRING	7
ecs-task-arn	O ARN da tarefa do ECS se o tráfego for proveniente de uma tarefa do ECS em execução. Para incluir esse campo na sua assinatura, você vai precisar de permissão para chamar ecs:ListClusters e ecs:ListTasks. Tipo de dados em Parquet: STRING	7
ecs-task-id	O ID da tarefa do ECS se o tráfego for proveniente de uma tarefa do ECS em execução. Para incluir esse campo na sua assinatura, você vai precisar de permissão para chamar ecs:ListClusters e ecs:ListTasks. Tipo de dados em Parquet: STRING	7

Campo	Descrição	Versão
rejeit-reason	Motivo da rejeição do tráfego. Valores possíveis: BPA. Retorna um '-' para qualquer outro motivo de rejeição. Para obter mais informações sobre o atributo Bloquear o Acesso Público (BPA) da VPC, consulte Bloquear o acesso público a VPCs e sub-redes. Tipo de dados em Parquet: STRING	8

Exemplos de registro de log de fluxo

Os exemplos a seguir mostram registros de log de fluxo que capturam fluxos de tráfego específicos.

Para obter informações sobre o formato de registro de log de fluxo, consulte Registros de log de fluxo. Para obter informações sobre como criar logs de fluxo, consulte Trabalhar com logs de fluxo.

Tópicos

- Tráfego aceito e rejeitado
- Sem dados e registros ignorados
- Regras de grupo de segurança e ACL de rede
- Tráfego IPv6
- Sequência de sinalizadores TCP
- Tráfego por meio de um gateway NAT
- Tráfego por meio de um gateway de trânsito
- Nome do serviço, caminho de tráfego e direção do fluxo

Tráfego aceito e rejeitado

Veja a seguir exemplos de registros de log de fluxo padrão.

Neste exemplo, o tráfego SSH (porta de destino 22, protocolo TCP) do endereço IP 172.31.16.139 para a interface de rede com endereço IP privado é 172.31.16.21 e o ID eni-1235b8ca123456789 na conta 123456789010 foi permitido.

```
2 123456789010 eni-1235b8ca123456789 172.31.16.139 172.31.16.21 20641 22 6 20 4249
 1418530010 1418530070 ACCEPT OK
```

Neste exemplo, o tráfego RDP (porta de destino 3389, protocolo TCP) para a interface de rede eni-1235b8ca123456789 na conta 123456789010 foi rejeitado.

```
2 123456789010 eni-1235b8ca123456789 172.31.9.69 172.31.9.12 49761 3389 6 20 4249
 1418530010 1418530070 REJECT OK
```

Sem dados e registros ignorados

Veja a seguir exemplos de registros de log de fluxo padrão.

Neste exemplo, nenhum dado foi registrado durante o intervalo de agregação.

```
2 123456789010 eni-1235b8ca123456789 - - - - - - - 1431280876 1431280934 - NODATA
```

Neste exemplo, os registros foram ignorados durante o intervalo de agregação. Os logs de fluxo da VPC ignoram registros que não conseguem capturar dados de logs de fluxo durante um intervalo de agregação porque excedem a capacidade interna. Um único registro ignorado pode representar vários fluxos que não foram capturados para a interface de rede durante o intervalo de agregação.

```
2 123456789010 eni-11111111aaaaaaaaa - - - - - - - 1431280876 1431280934 - SKIPDATA
```

> **Note**
>
> Alguns registros de log de fluxo podem ser ignorados durante o intervalo de agregação (consulte log-status em Campos disponíveis). Isso pode ocorrer em virtude de uma restrição de capacidade interna da AWS ou de um erro interno. Se você estiver usando o AWS Cost Explorer para visualizar as cobranças dos logs de fluxo da VPC e alguns logs de fluxo forem ignorados durante o intervalo de agregação de logs de fluxo, o número de logs de fluxo relatados AWS Cost Explorer será maior do que o número de logs de fluxo publicados pela Amazon VPC.

Regras de grupo de segurança e ACL de rede

Se você estiver usando logs de fluxo para diagnosticar regras de grupo de segurança ou regras de ACL de rede exageradamente restritivas ou permissivas, fique atento ao estado desses recursos. Os grupos de segurança são com estado. Isso significa que as respostas ao tráfego permitido

são também permitidas, mesmo que as regras em seu grupo de segurança não permitam isso. Inversamente, as ACLs de rede são stateless e, portanto, as respostas ao tráfego permitido estão sujeitas a regras de ACL de rede.

Por exemplo, você usa o comando ping em seu computador doméstico (o endereço IP é 203.0.113.12) para a sua instância (o endereço IP privado da interface de rede é 172.31.16.139). As regras de entrada do grupo de segurança permitem tráfego ICMP, mas as regras de saída não permitem tráfego ICMP. Como os grupos de segurança são com estado, o ping de resposta da sua instância é permitido. Sua ACL de rede permite tráfego ICMP de entrada, mas não permite tráfego ICMP de saída. Como as ACLs de rede são stateless, o ping de resposta é interrompido e não chega ao seu computador doméstico. Em um log de fluxo padrão, isso é exibido como dois registros de log de fluxo:

- Um registro ACCEPT para o ping originário foi permitido tanto pela ACL de rede quanto pelo grupo de segurança e, por isso, obteve permissão para acessar sua instância.
- Um registro REJECT para o ping de resposta que a ACL de rede negou.

```
2 123456789010 eni-1235b8ca123456789 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027
 1432917142 ACCEPT OK
```

```
2 123456789010 eni-1235b8ca123456789 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094
 1432917142 REJECT OK
```

Se sua ACL de rede permitir tráfego ICMP de saída, o log de fluxo exibirá dois registros ACCEPT (um para o ping originário e outro para o ping de resposta). Se seu grupo de segurança negar tráfego ICMP de entrada, o log de fluxo exibirá um único registro REJECT, porque o tráfego não recebeu permissão para acessar sua instância.

Tráfego IPv6

Veja a seguir um exemplo de um registro de log de fluxo padrão. No exemplo, o tráfego SSH (porta 22) do endereço IPv6 2001:db8:1234:a100:8d6e:3477:df66:f105 para a interface de rede eni-1235b8ca123456789 na conta 123456789010 foi permitido.

```
2 123456789010 eni-1235b8ca123456789 2001:db8:1234:a100:8d6e:3477:df66:f105
 2001:db8:1234:a102:3304:8879:34cf:4071 34892 22 6 54 8855 1477913708 1477913820 ACCEPT
 OK
```

Sequência de sinalizadores TCP

Esta seção inclui exemplos de logs de fluxo personalizados que capturam os campos a seguir, na ordem abaixo.

```
version vpc-id subnet-id instance-id interface-id account-id type srcaddr dstaddr
 srcport dstport pkt-srcaddr pkt-dstaddr protocol bytes packets start end action tcp-
flags log-status
```

O campo tcp-flags nos exemplos desta seção é representado pelo penúltimo valor no log de fluxo. Sinalizadores TCP podem ajudar você a identificar a direção do tráfego como, por exemplo, qual servidor iniciou a conexão.

> **Note**
>
> Para saber mais sobre a opção tcp-flags e obter uma explicação de cada um dos sinalizadores TCP, consulte Campos disponíveis.

Nos registros a seguir (que começam às 19:47:55 e terminam às 19:48:53), as duas conexões foram iniciadas por um cliente em um servidor em execução na porta 5001. Dois sinalizadores SYN (2) foram recebidos pelo servidor do cliente de portas de origem diferentes no cliente (43416 e 43418). Para cada SYN, um SYN-ACK foi enviado do servidor para o cliente (18) na porta correspondente.

```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43416 5001
 52.213.180.42 10.0.0.62 6 568 8 1566848875 1566848933 ACCEPT 2 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43416 10.0.0.62
 52.213.180.42 6 376 7 1566848875 1566848933 ACCEPT 18 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43418 5001
 52.213.180.42 10.0.0.62 6 100701 70 1566848875 1566848933 ACCEPT 2 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43418 10.0.0.62
 52.213.180.42 6 632 12 1566848875 1566848933 ACCEPT 18 OK
```

No segundo intervalo de agregação, uma das conexões que foi estabelecida durante o fluxo anterior agora está fechada. O cliente enviou um sinalizador FIN (1) para o servidor para a conexão na porta 43418. O servidor enviou um FIN para o cliente na porta 43418.

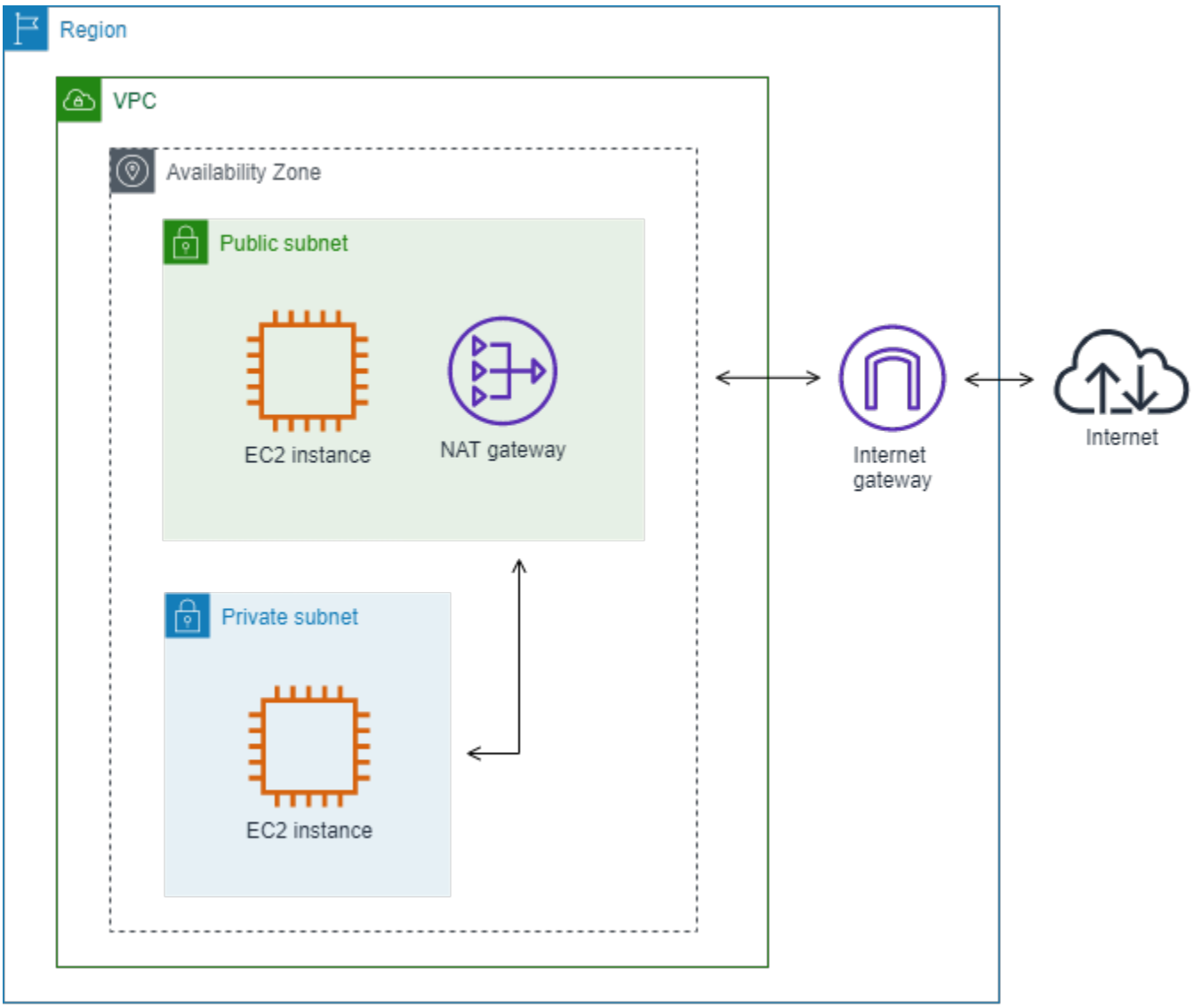
```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43418 10.0.0.62
 52.213.180.42 6 63388 1219 1566848933 1566849113 ACCEPT 1 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43418 5001
 52.213.180.42 10.0.0.62 6 23294588 15774 1566848933 1566849113 ACCEPT 1 OK
```

Para conexões curtas (por exemplo, alguns segundos) que são abertas e fechadas em um único intervalo de agregação, os sinalizadores podem ser definidos na mesma linha no registro de log do fluxo de tráfego na mesma direção. No exemplo a seguir, a conexão é estabelecida e finalizada no mesmo intervalo de agregação. Na primeira linha, o valor do sinalizador TCP é 3, que indica o envio de um SYN e de uma mensagem FIN do cliente para o servidor. Na segunda linha, o valor do sinalizador TCP é 19, que indica o envio de um SYN-ACK e de uma mensagem FIN do servidor para o cliente.

```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43638 5001
 52.213.180.42 10.0.0.62 6 1260 17 1566933133 1566933193 ACCEPT 3 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43638  10.0.0.62
 52.213.180.42 6 967 14 1566933133 1566933193 ACCEPT 19 OK
```

Tráfego por meio de um gateway NAT

Neste exemplo, uma instância em uma sub-rede privada acessa a Internet por meio de um gateway NAT que está em uma sub-rede pública.



O log de fluxo personalizado a seguir para a interface de rede do gateway NAT captura os seguintes campos nesta ordem.

```
instance-id interface-id srcaddr dstaddr pkt-srcaddr pkt-dstaddr
```

O log de fluxo mostra o fluxo do tráfego do endereço IP da instância (10.0.1.5) por meio da interface de rede do gateway NAT para um host na Internet (203.0.113.5). A interface de rede do gateway NAT é uma interface de rede gerenciada pelo solicitante e, portanto, o registro de log de fluxo exibe um símbolo “-” para o campo instance-id. A linha a seguir mostra o tráfego da instância de origem para a interface de rede do gateway NAT. Os valores dos campos dstaddr e pkt-dstaddr são diferentes. O campo dstaddr exibe o endereço IP privado da interface de rede do gateway NAT, e o campo pkt-dstaddr exibe o endereço IP de destino final do host na Internet.

```
- eni-1235b8ca123456789 10.0.1.5 10.0.0.220 10.0.1.5 203.0.113.5
```

As duas próximas linhas mostram o tráfego da interface de rede do gateway NAT para o host de destino na Internet e o tráfego de resposta do host para a interface de rede do gateway NAT.

```
- eni-1235b8ca123456789 10.0.0.220 203.0.113.5 10.0.0.220 203.0.113.5
- eni-1235b8ca123456789 203.0.113.5 10.0.0.220 203.0.113.5 10.0.0.220
```

A linha a seguir mostra o tráfego de resposta da interface de rede do gateway NAT para a instância de origem. Os valores dos campos srcaddr e pkt-srcaddr são diferentes. O campo srcaddr exibe o endereço IP privado da interface de rede do gateway NAT, e o campo pkt-srcaddr exibe o endereço IP do host na Internet.

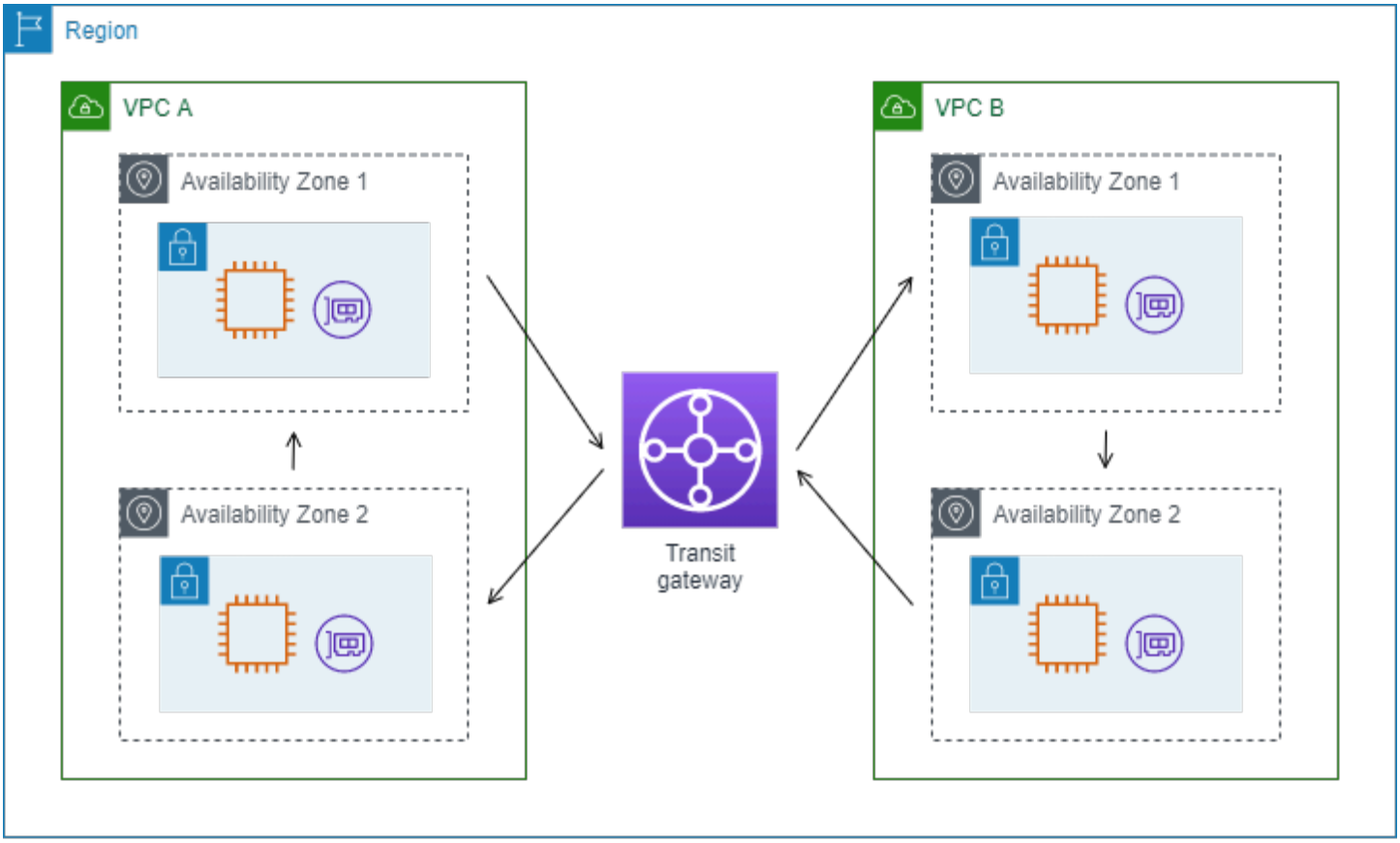
```
- eni-1235b8ca123456789 10.0.0.220 10.0.1.5 203.0.113.5 10.0.1.5
```

Você cria outro log de fluxo personalizado usando o mesmo conjunto de campos acima. Você cria o log de fluxo da interface de rede para a instância na sub-rede privada. Nesse caso, o campo instance-id retorna o ID da instância que se associa à interface de rede, e não há diferença entre os campos dstaddr e pkt-dstaddr e os campos srcaddr e pkt-srcaddr. Diferente da interface de rede do gateway NAT, essa interface de rede não é intermediária para tráfego.

```
i-01234567890123456 eni-1111aaaa2222bbbb3 10.0.1.5 203.0.113.5 10.0.1.5 203.0.113.5
 #Traffic from the source instance to host on the internet
i-01234567890123456 eni-1111aaaa2222bbbb3 203.0.113.5 10.0.1.5 203.0.113.5 10.0.1.5
 #Response traffic from host on the internet to the source instance
```

Tráfego por meio de um gateway de trânsito

Neste exemplo, um cliente na VPC A se conecta a um servidor da Web na VPC B por meio de um gateway de trânsito. O cliente e o servidor estão em zonas de disponibilidade diferentes. O tráfego chega no servidor na VPC B utilizando um ID de interface de rede elástica (neste exemplo, vamos supor que o ID seja eni-11111111111111111111) e sai do VPC B utilizando outro (por exemplo, eni-222222222222222).



Você cria um log de fluxo personalizado para a VPC B com o seguinte formato.

```
version interface-id account-id vpc-id subnet-id instance-id srcaddr dstaddr srcport
 dstport protocol tcp-flags type pkt-srcaddr pkt-dstaddr action log-status
```

As linhas a seguir dos registros de log de fluxo demonstram o fluxo de tráfego na interface de rede para o servidor da Web. A primeira linha é o tráfego de solicitação do cliente e a última linha é o tráfego de resposta do servidor da Web.

```
3 eni-33333333333333333 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb
 i-01234567890123456 10.20.33.164 10.40.2.236 39812 80 6 3 IPv4 10.20.33.164
 10.40.2.236 ACCEPT OK
...
3 eni-33333333333333333 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb
 i-01234567890123456 10.40.2.236 10.20.33.164 80 39812 6 19 IPv4 10.40.2.236
 10.20.33.164 ACCEPT OK
```

A linha a seguir é o tráfego de solicitação na eni-11111111111111111, uma interface de rede gerenciada pelo solicitante para o gateway de trânsito na sub-rede subnet-11111111aaaaaaaaa. O

registro de log de fluxo exibe, portanto, um símbolo “-” para o campo instance-id. O campo srcaddr exibe o endereço IP privado da interface de rede de gateway de trânsito, e o campo pkt-srcaddr exibe o endereço IP de origem do cliente na VPC A.

```
3 eni-11111111111111111 123456789010 vpc-abcdefab012345678 subnet-11111111aaaaaaaaa -
 10.40.1.175 10.40.2.236 39812 80 6 3 IPv4 10.20.33.164 10.40.2.236 ACCEPT OK
```

A linha a seguir é o tráfego de solicitação na eni-22222222222222222, uma interface de rede gerenciada pelo solicitante para o gateway de trânsito na sub-rede subnet-22222222bbbbbbbbb. O campo dstaddr exibe o endereço IP privado da interface de rede de gateway de trânsito, e o campo pkt-dstaddr exibe o endereço IP do cliente na VPC A.

```
3 eni-22222222222222222 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb -
 10.40.2.236 10.40.2.31 80 39812 6 19 IPv4 10.40.2.236 10.20.33.164 ACCEPT OK
```

Nome do serviço, caminho de tráfego e direção do fluxo

Veja a seguir um exemplo dos campos para um registro de log de fluxo personalizado.

```
version srcaddr dstaddr srcport dstport protocol start end type packets bytes account-
id vpc-id subnet-id instance-id interface-id region az-id sublocation-type sublocation-
id action tcp-flags pkt-srcaddr pkt-dstaddr pkt-src-aws-service pkt-dst-aws-service
 traffic-path flow-direction log-status
```

No exemplo a seguir, a versão é a 5 porque os registros incluem campos da versão 5. Uma instância do EC2 aciona o serviço do Amazon S3. Os logs de fluxo são capturados na interface de rede para a instância. O primeiro registro tem uma direção de fluxo de ingress e o segundo, uma direção de fluxo de egress. Para o registro egress, o traffic-path é 8, indicando que o tráfego passa por um gateway da Internet. O campo traffic-path não é compatível com o tráfego ingress. Quando pkt-srcaddr ou pkt-dstaddr for um endereço IP público, o nome do serviço será exibido.

```
5 52.95.128.179 10.0.0.71 80 34210 6 1616729292 1616729349 IPv4 14 15044
 123456789012 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-0c50d5961bcb2d47b
 eni-1235b8ca123456789 ap-southeast-2 apse2-az3 - - ACCEPT 19 52.95.128.179 10.0.0.71
 S3 - - ingress OK
5 10.0.0.71 52.95.128.179 34210 80 6 1616729292 1616729349 IPv4 7 471 123456789012 vpc-
abcdefab012345678 subnet-aaaaaaaa012345678 i-0c50d5961bcb2d47b eni-1235b8ca123456789
 ap-southeast-2 apse2-az3 - - ACCEPT 3 10.0.0.71 52.95.128.179 - S3 8 egress OK
```

Limitações do log de fluxo

Para usar logs de fluxo, você precisa estar atento às seguintes limitações:

- Após criar um log de fluxo, você não verá os dados do log de fluxo até que haja tráfego ativo para a interface de rede, sub-rede ou VPC que você selecionou.
- Você não pode habilitar logs de fluxo para VPCs emparelhadas com a sua VPC, a menos que a VPC emparelhada esteja em sua conta.
- Após criar um log de fluxo, não é possível alterar sua configuração ou o formato do registro do log de fluxo. Por exemplo, não é possível associar uma função do IAM diferente ao log de fluxo, nem adicionar ou remover campos no registro do log de fluxo. Em vez disso, você pode excluir o log de fluxo e criar um novo com a configuração necessária.
- Se sua interface de rede tiver vários endereços IPv4 e o tráfego for enviado para um endereço IPv4 privado secundário, o log de fluxo exibirá o endereço IPv4 privado primário no campo `dstaddr`. Para capturar o endereço IP de destino original, crie um log de fluxo com o campo `pkt-dstaddr`.
- Se o tráfego for enviado para uma interface de rede e o destino não for nenhum dos endereços IP da interface de rede, o log de fluxo exibirá o endereço IPv4 privado principal no campo `dstaddr`. Para capturar o endereço IP de destino original, crie um log de fluxo com o campo `pkt-dstaddr`.
- Caso o tráfego seja enviado de uma interface de rede e a origem não corresponda a nenhum dos endereços IP dessa interface de rede, quando o registro de log for referente a um fluxo de saída, o log mostrará o endereço IPv4 privado principal no campo `srcaddr`. Para capturar o endereço IP de origem original, crie um log de fluxo com o campo `pkt-srcaddr`. Caso o registro de log seja para um fluxo de entrada na interface de rede, o endereço IP privado principal da interface de rede não será mostrado no campo `srcaddr`.
- Quando uma interface de rede é anexada a uma instância baseada em Nitro, o intervalo de agregação é sempre 1 minuto ou menos, independentemente do intervalo de agregação máximo especificado.
- Para os campos `pkt-srcaddr` e `pkt-dstaddr`, se a camada intermediária tiver a Preservação do endereço IP do cliente ativada, esse campo poderá mostrar o IP do cliente preservado, em vez do endereço IP da camada intermediária.
- Alguns registros de log de fluxo podem ser ignorados durante o intervalo de agregação (consulte log-status em Campos disponíveis). Isso pode ocorrer em virtude de uma restrição de capacidade interna da AWS ou de um erro interno. Se você estiver usando o AWS Cost Explorer para visualizar as cobranças dos logs de fluxo da VPC e alguns logs de fluxo forem ignorados durante

o intervalo de agregação de logs de fluxo, o número de logs de fluxo relatados AWS Cost Explorer será maior do que o número de logs de fluxo publicados pela Amazon VPC.

- Se você estiver usando o atributo Bloquear o Acesso Público (BPA) da VPC:
  - Os logs de fluxo para o BPA da VPC não incluem os registros ignorados.
  - Os logs de fluxo para o BPA da VPC não incluem `bytes` mesmo que você inclua o campo `bytes` no log de fluxo.

Os logs de fluxo não capturam todo o tráfego de IP. Os tipos de tráfego a seguir não são registrados:

- O tráfego gerado por instâncias quando elas entram em contato com o servidor de DNS da Amazon. Se você usar seu próprio servidor de DNS, todo tráfego para esse servidor de DNS será registrado.
- O tráfego gerado por uma instância Windows para ativação de licença do Amazon Windows.
- O tráfego para e proveniente de `169.254.169.254` para metadados de instância.
- O tráfego para e proveniente de `169.254.169.123` para o Amazon Time Sync Service.
- Tráfego DHCP.
- Tráfego de origem do tráfico espelhado. Você só verá tráfego de destino do tráfego espelhado.
- Tráfego para o endereço IP reservado para o router padrão da VPC.
- Trafegue entre uma interface de rede do endpoint e uma interface de rede do Network Load Balancer.
- Tráfego do Protocolo de Resolução de Endereço (ARP).

Limitações específicas dos campos do ECS disponíveis na versão 7:

- Para criar assinaturas de log de fluxo com campos do ECS, sua conta deve conter pelo menos um cluster do ECS.
- Os campos do ECS não serão computados se as tarefas subjacentes do ECS não pertencerem ao proprietário da assinatura do log de fluxo. Por exemplo, se você compartilhar uma sub-rede (`SubnetA`) com outra conta (`AccountB`) e, em seguida, criar uma assinatura de log de fluxo para a `SubnetA`, se `AccountB` iniciar tarefas do ECS na sub-rede compartilhada, sua assinatura receberá logs de tráfego das tarefas do ECS iniciadas por `AccountB`, mas os campos do ECS desses logs não serão calculados devido a questões de segurança.
- Se você criar assinaturas de log de fluxo com campos do ECS no nível de recurso de VPC/sub-rede, qualquer tráfego gerado para interfaces de rede não pertencentes ao ECS também

será entregue para suas assinaturas. Os valores dos campos do ECS serão "-" para tráfego IP não pertencente ao ECS. Por exemplo, você tem uma sub-rede (`subnet-000000`) e cria uma assinatura de log de fluxo para essa sub-rede com campos do ECS (`fl-00000000`). Na `subnet-000000`, você executa uma instância do EC2 (`i-0000000`) que está conectada à Internet e está gerando ativamente tráfego IP. Você também inicia uma tarefa do ECS em execução (`ECS-Task-1`) na mesma sub-rede. Como ambos `i-0000000` e `ECS-Task-1` estão gerando tráfego IP, sua assinatura de log de fluxo `fl-00000000` fornecerá logs de tráfego para ambas as entidades. No entanto, só `ECS-Task-1` terá metadados efetivos do ECS para os campos do ECS que você incluiu em seu logFormat. Para tráfego relacionado a `i-0000000`, esses campos terão um valor de "-".

- `ecs-container-id` e `ecs-second-container-id` são ordenados à medida que o serviço VPC Flow Logs recebê-los do fluxo de eventos do ECS. Não há garantias de que eles estarão na mesma ordem em que você os vê no console do ECS ou na chamada de API DescribetAsk. Se um contêiner entrar no status PARADO enquanto a tarefa ainda estiver em execução, ela poderá continuar aparecendo no seu log.
- Os metadados do ECS e os registros de tráfego IP são provenientes de duas origens diferentes. Começaremos a computar seu tráfego do ECS assim que obtivermos todas as informações necessárias das dependências upstream. Depois que você inicia uma nova tarefa, começaremos a calcular seus campos do ECS 1) quando recebermos tráfego IP para a interface de rede subjacente e 2) quando recebermos o evento do ECS contendo os metadados da sua tarefa do ECS para indicar que a tarefa está em execução. Depois que você interromper uma tarefa, vamos parar de calcular seus campos do ECS 1) quando não recebermos mais tráfego IP para a interface de rede subjacente ou recebermos tráfego IP atrasado por mais de um dia e 2) quando recebermos o evento do ECS contendo os metadados da sua tarefa do ECS para indicar que a tarefa não está mais em execução.
- Só há compatibilidade com tarefas do ECS iniciadas no modo de rede `awsvpc`.

Preços

As cobranças de ingestão e de arquivamento de dados para logs fornecidos se aplicam quando você publica logs de fluxo. Para obter mais informações sobre preços ao publicar logs fornecidos, abra Amazon CloudWatch Pricing (Preços do Amazon CloudWatch), selecione Logs e encontre Vended Logs (Logs fornecidos).

Para rastrear cobranças da publicação de logs de fluxo, você pode aplicar tags de alocação de custos ao recurso de destino. Em seguida, o relatório de alocação de custos da AWS incluirá o uso e

os custos agregados por essas tags. É possível aplicar tags que representem categorias de negócios (como centros de custos, nomes de aplicativos ou proprietários) para organizar os custos. Para obter mais informações, consulte:

- Usar tags de alocação de custos no Guia do usuário do AWS Billing.
- Tag log groups in Amazon CloudWatch Logs (Marcar grupos de logs no Amazon CloudWatch Logs) no Amazon CloudWatch Logs User Guide (Guia do usuário do Amazon CloudWatch Logs)
- Using cost allocation S3 bucket tags (Usar tags de alocação de custos para buckets do S3) no Amazon Simple Storage Service User Guide (Guia do usuário do Amazon Simple Storage Service)
- Marcar fluxos de entrega no Guia do desenvolvedor do Amazon Data Firehose

Trabalhar com logs de fluxo

É possível trabalhar com logs de fluxo usando os consoles do Amazon EC2 e da Amazon VPC.

Tarefas

- 1. Controlar o uso de logs de fluxo com o IAM
- 2. Criar um log de fluxo
- 3. Marcar um log de fluxo
- 4. Excluir um log de fluxo
- Visão geral da linha de comando

1. Controlar o uso de logs de fluxo com o IAM

Por padrão, os usuários do não têm permissão para trabalhar com logs de fluxo. É possível criar um perfil do IAM com uma política anexada que conceda permissões aos usuários para criar, descrever e excluir logs de fluxo.

Veja a seguir uma política de exemplo que concede aos usuários as permissões totais para criar, descrever e excluir logs de fluxo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```
        "ec2:DeleteFlowLogs",
        "ec2:CreateFlowLogs",
        "ec2:DescribeFlowLogs"
      ],
      "Resource": "*"
    }
  ]
}
```

Para ter mais informações, consulte the section called “Como a Amazon VPC funciona com o IAM”.

2. Criar um log de fluxo

É possível criar logs de fluxos para suas VPCs, sub-redes ou interfaces de rede. Ao criar um log de fluxo, você deve especificar um destino para o log de fluxo. Para obter mais informações, consulte:

- the section called “Criar um log de fluxo que publique no CloudWatch Logs”
- the section called “Criar um log de fluxo para publicação no Amazon S3”
- the section called “Criar um log de fluxo para publicação no Amazon Data Firehose”

3. Marcar um log de fluxo

Você pode adicionar ou remover tags de um log de fluxo a qualquer momento.

Para gerenciar tags para um log de fluxo

1. Execute um destes procedimentos:
   - Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/. No painel de navegação, selecione Network Interfaces. Marque a caixa de seleção para a interface de rede.
   - Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/. No painel de navegação, escolha Your VPCs (Suas VPCs). Marque a caixa de seleção da VPC.
   - Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/. No painel de navegação, escolha Sub-redes. Marque a caixa de seleção da sub-rede.
2. Escolha Flow Logs.(Logs de fluxo).
3. Selecione Ações, Gerenciar tags.
4. Para adicionar uma nova tag, escolha Add new tag (Adicionar nova tag) e insira a chave e o valor da tag. Para remover uma tag, selecione Remover.

5. Ao finalizar a adição ou a remoção de tags, escolha Save (Salvar).

4. Excluir um log de fluxo

É possível excluir um log de fluxo a qualquer momento. Depois que você exclui um log de fluxo, pode levar vários minutos para a coleta de dados se encerrar.

A exclusão de um log de fluxo não exclui os dados do log do destino nem modifica o recurso de destino. Você deve excluir os dados do log de fluxo existente diretamente no destino e limpar o recurso de destino usando o console do serviço de destino.

Para excluir um log de fluxo

1. Execute um destes procedimentos:
   - Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/. No painel de navegação, selecione Network Interfaces. Marque a caixa de seleção para a interface de rede.
   - Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/. No painel de navegação, escolha Your VPCs (Suas VPCs). Marque a caixa de seleção da VPC.
   - Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/. No painel de navegação, escolha Sub-redes. Marque a caixa de seleção da sub-rede.
2. Escolha Flow Logs.(Logs de fluxo).
3. Escolha Actions, (Ações), Delete flow logs (Excluir logs de fluxo).
4. Quando a confirmação for solicitada, insira **`delete`** e escolha Delete (Excluir).

Visão geral da linha de comando

É possível executar as tarefas descritas nesta página por meio da linha de comando.

Criar um log de fluxos

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

Descrever um log de fluxo

- describe-flow-logs (AWS CLI)

- Get-EC2FlowLog (AWS Tools for Windows PowerShell)

Marcar um log de fluxo

- create-tags and delete-tags (AWS CLI)
- New-EC2Tag e Remove-EC2Tag (AWS Tools for Windows PowerShell)

Excluir um log de fluxo

- delete-flow-logs (AWS CLI)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)

Publicar logs de fluxo no CloudWatch Logs

Os logs de fluxos podem publicar os dados de log de fluxos diretamente no Amazon CloudWatch. O Amazon CloudWatch é um serviço abrangente de monitoramento e observabilidade. Ele coleta e rastreia métricas, registros e dados de eventos de vários recursos da AWS, bem como de seus serviços e aplicações. O CloudWatch fornece visibilidade sobre a utilização de recursos, performance de aplicações e integridade operacional, permitindo detectar e responder a mudanças na performance e a possíveis problemas em todo o sistema. Com o CloudWatch, você pode definir alarmes, visualizar registros e métricas e reagir automaticamente para coletar e otimizar seus recursos na nuvem. Ele é uma ferramenta essencial para garantir a confiabilidade, a disponibilidade e a performance da infraestrutura e das aplicações baseadas na nuvem.

Ao publicar no CloudWatch Logs, os dados de log de fluxo são publicados em um grupo de logs, e cada interface de rede tem um stream de logs exclusivo no grupo de logs. Os fluxos de log contêm registros de log de fluxo. Você pode criar vários logs de fluxo que publicam dados no mesmo grupo de logs. Se houver uma mesma interface de rede em um ou mais logs de fluxo no mesmo grupo de logs, haverá um stream misto de logs. Se tiver especificado que um log de fluxo deve capturar tráfego rejeitado e outro log de fluxo deve capturar o tráfego aceito, o stream misto de logs capturará todos os tráfegos.

No CloudWatch Logs, o campo timestamp (carimbo de data/hora) corresponde à hora de início capturada no registro de log do fluxo. O campo ingestionTime (Tempo de consumo) indica a data e a hora em que o registro de log do fluxo foi recebido pelo CloudWatch Logs. Esse timestamp é posterior à hora de término capturada no registro de log do fluxo.

Para obter mais informações sobre o CloudWatch Logs, consulte Logs sent to CloudWatch Logs (Logs enviados ao CloudWatch Logs) no Guia do usuário do Amazon CloudWatch Logs.

Preços

As cobranças de arquivamento e ingestão de dados para logs vendidos se aplicam quando você publica logs de fluxos no CloudWatch Logs. Para obter mais informações, abra Amazon CloudWatch Pricing (Preços do Amazon CloudWatch), selecione Logs e encontre Vended Logs (Logs fornecidos).

Conteúdo

Perfil do IAM para publicar logs de fluxo no CloudWatch Logs

A função do IAM associada ao log de fluxo deve ter permissões suficientes para publicar logs de fluxo para o grupo de logs especificado no CloudWatch Logs. A função do IAM deve pertencer à sua conta da AWS.

A política do IAM anexada à sua função do IAM deve incluir pelo menos as permissões a seguir.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
    }
  ]
```

```
}
```

Verifique se a sua função tem a política de confiança a seguir, que permite que o serviço de logs de fluxo assuma a função.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Recomendamos o uso das chaves de condição `aws:SourceAccount` e `aws:SourceArn` para se proteger contra O problema do agente confuso. Por exemplo, você poderia adicionar o bloco de condições a seguir na política de confiança anterior. A conta de origem é o proprietário do log de fluxo e o ARN de origem é o ARN do log de fluxo. Se você não souber o ID do log de fluxos, poderá substituir essa parte do ARN por um caractere curinga (*) e, em seguida, atualizar a política depois de criar o log de fluxos.

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:region:account_id:vpc-flow-log/flow-log-id"
    }
}
```

Criar um perfil do IAM para logs de fluxo

Você pode atualizar um perfil existente conforme descrito acima. Como alternativa, você pode usar o seguinte procedimento para criar um novo perfil para usar com os logs de fluxo. Você especificará esse perfil ao criar o log de fluxo.

Como criar um perfil do IAM para logs de fluxos

1. Abra o console do IAM, em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Policies.
3. Selecione Criar política.
4. Na página Create policy (Criar política) faça o seguinte:
   a. Escolha JSON.
   b. Substitua o conteúdo dessa janela pela política de permissões no início desta seção.
   c. Escolha Próximo.
   d. Insira um nome e uma descrição e tags opcionais para a política e escolha Criar política.
5. No painel de navegação, selecione Perfis.
6. Escolha Criar Perfil.
7. Em Trusted entity type (Tipo de entidade confiável), escolha Custom trust policy (Política de confiança personalizada). Em Custom trust policy (Política de confiança personalizada), substitua `"Principal": {},` pelo seguinte e escolha Next (Próximo).

```
"Principal": {
   "Service": "vpc-flow-logs.amazonaws.com"
},
```

8. Na página Add permissions (Adicionar permissões), marque a caixa de seleção correspondente à política que você criou anteriormente neste procedimento e, em seguida, escolha Next (Próximo).
9. Insira um nome para a função e, opcionalmente, uma descrição.
10. Selecione Criar perfil.

Criar um log de fluxo que publique no CloudWatch Logs

É possível criar logs de fluxos para suas VPCs, sub-redes ou interfaces de rede. Caso execute essas etapas como um usuário usando um perfil do IAM específico, verifique se o perfil tem permissões para usar a ação `iam:PassRole`.

Pré-requisito

Verifique se a entidade principal do IAM que você está usando para fazer a solicitação tem permissões para chamar a ação `iam:PassRole`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["iam:PassRole"],
      "Resource": "arn:aws:iam::account-id:role/flow-log-role-name"
    }
  ]
}
```

Para criar um log de fluxo usando o console

1. Execute um destes procedimentos:
   - Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/. No painel de navegação, selecione Network Interfaces. Marque a caixa de seleção para a interface de rede.
   - Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/. No painel de navegação, escolha Your VPCs (Suas VPCs). Marque a caixa de seleção da VPC.
   - Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/. No painel de navegação, escolha Sub-redes. Marque a caixa de seleção da sub-rede.
2. Selecione Ações, Criar log de fluxo.
3. Em Filter (Filtrar), especifique o tipo de tráfego a ser registrado em log. Selecione All (Todos) para registrar em log o tráfego aceito e rejeitado, Rejected (Rejeitado) para registrar somente o tráfego rejeitado ou Accepted (Aceito) para registrar somente o tráfego aceito.
4. Em Maximum aggregation interval (Intervalo máximo de agregação), escolha o período máximo durante o qual um fluxo é capturado e agregado em um registro de log de fluxo.
5. Para Destination (Destino), escolha Send to CloudWatch Logs (Enviar para o CloudWatch Logs).
6. Em Grupo de logs de destino, escolha o nome de um grupo de logs existente ou insira o nome de um novo grupo de logs. Se você inserir um nome, criaremos o grupo de registros quando houver tráfego para registrar em log.
7. Para o Acesso ao serviço, escolha um perfil de serviço do IAM existente que tenha permissões para publicar logs no CloudWatch Logs ou escolha criar um novo perfil de serviço.
8. Em Formato de registro do log , selecione o formato para o registro de log de fluxo.
   - Para usar o formato padrão, escolha AWS Formato padrão.

- Para usar um formato personalizado, escolha Formato personalizado e, em seguida, selecione os campos de Formato de log.

9. Para Metadados adicionais, escolha se quer incluir metadados do Amazon ECS no formato de log.
10. (Opcional) Selecione Adicionar nova tag para aplicar tags ao log de fluxo.
11. Selecione Criar log de fluxo.

Como criar um log de fluxo usando a linha de comando

Use um dos seguintes comandos.

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

O exemplo de AWS CLI a seguir cria um log de fluxo que captura todo o tráfego aceito para a sub-rede especificada. Os logs de fluxo são entregues ao grupo de logs especificado. O parâmetro `--deliver-logs-permission-arn` especifica o perfil do IAM necessário para publicar no CloudWatch Logs.

```
aws ec2 create-flow-logs --resource-type Subnet --resource-ids subnet-1a2b3c4d --
traffic-type ACCEPT --log-group-name my-flow-logs --deliver-logs-permission-arn
 arn:aws:iam::123456789101:role/publishFlowLogs
```

Visualizar registros de log de fluxo com o CloudWatch Logs

É possível visualizar os registros dos logs de fluxo por meio do console do CloudWatch Logs. Depois que o log de fluxo é criado, pode levar alguns minutos para ele ficar visível no console.

Para visualizar registros de log de fluxo publicados no CloudWatch Logs

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Logs, Grupos de log.
3. Selecione o nome do grupo de logs que contém os logs de fluxo para abrir a página de detalhes.
4. Selecione o nome do fluxo de logs que contém os registros de log de fluxo. Para ter mais informações, consulte Registros de log de fluxo.

Para visualizar registros de log de fluxo publicados no CloudWatch Logs usando a linha de comando

- get-log-events (AWS CLI)
- Get-CWLLogEvent (AWS Tools for Windows PowerShell)

Procurar registros de log de fluxo

É possível pesquisar os registros de log de fluxo publicados no CloudWatch Logs usando o console do CloudWatch Logs. Os filtros de métrica podem ser usados para filtrar registros de log de fluxo. Os registros de log de fluxo são delimitados por espaço.

Como pesquisar registros de log de fluxo usando o console do CloudWatch Logs

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Logs, Grupos de log.
3. Selecione o grupo de logs que contém o log de fluxo e, em seguida, selecione o fluxo de logs se você souber a interface de rede que está pesquisando. Como alternativa, escolha Search log group (Pesquisar grupo de logs). Isso pode levar algum tempo se houver muitas interfaces de rede no grupo de logs ou dependendo do intervalo de tempo selecionado.
4. Em Filtrar eventos, insira a sequência abaixo. Isso pressupõe que o registro de log de fluxo usa o formato padrão.

   ```
   [version, accountid, interfaceid, srcaddr, dstaddr, srcport, dstport, protocol,
    packets, bytes, start, end, action, logstatus]
   ```

5. Modifique o filtro conforme necessário especificando valores para os campos. Os exemplos a seguir filtram por endereços IP de origem específicos.

   ```
   [version, accountid, interfaceid, srcaddr = 10.0.0.1, dstaddr, srcport, dstport,
    protocol, packets, bytes, start, end, action, logstatus]
   [version, accountid, interfaceid, srcaddr = 10.0.2.*, dstaddr, srcport, dstport,
    protocol, packets, bytes, start, end, action, logstatus]
   ```

   Os exemplos a seguir filtram por porta de destino, número de bytes e se o tráfego foi rejeitado.

   ```
   [version, accountid, interfaceid, srcaddr, dstaddr, srcport, dstport = 80 ||
    dstport = 8080, protocol, packets, bytes, start, end, action, logstatus]
   ```

```
[version, accountid, interfaceid, srcaddr, dstaddr, srcport, dstport = 80 ||
 dstport = 8080, protocol, packets, bytes >= 400, start, end, action = REJECT,
 logstatus]
```

Processar registros de log de fluxo no CloudWatch Logs

É possível processar registros de log de fluxo do mesmo modo que você trabalharia com outros eventos de coletados pelo CloudWatch Logs. Para obter mais informações sobre como monitorar dados de log e filtros de métricas, consulte Creating metrics from log events using filter no Guia do usuário do Amazon CloudWatch Logs.

Exemplo: criação de um filtro de métricas no CloudWatch e um alarme para um log de fluxo

Neste exemplo, há um log de fluxo para `eni-1a2b3c4d`. Pode ser útil criar um alarme que o alerte se houver 10 ou mais tentativas rejeitadas de conexão à sua instância pela porta TCP 22 (SSH) no período de 1 hora. Primeiro, você deve criar um filtro de métrica que corresponda ao padrão do tráfego para o qual o alarme será criado. Depois, você pode criar um alarme para o filtro de métricas.

Como criar um filtro de métricas para tráfego SSH rejeitado e um alarme para o filtro

1. Abra o console do CloudWatch, em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Logs, Log groups (Grupos de log).
3. Marque a caixa de seleção do grupo de log e, em seguida, escolha Actions (Ações), Create metric filter (Criar filtro de métrica).
4. Em Filter Pattern (Padrão de filtro), insira a seguinte string.

```
[version, account, eni, source, destination, srcport, destport="22", protocol="6",
 packets, bytes, windowstart, windowend, action="REJECT", flowlogstatus]
```

5. Em Select Log Data to Test (Selecionar dados de log para teste), selecione o fluxo de logs da interface de rede. (Opcional) Para visualizar as linhas de dados de log que correspondem ao padrão do filtro, escolha Test Pattern (Padrão de teste).
6. Quando estiver pronto, selecione Avançar.
7. Insira um nome de filtro, um namespace de métrica e o nome da métrica. Defina o valor da métrica como 1. Quando terminar, escolha Next (Avançar) e, em seguida, escolha Create metric filter (Criar filtro de métrica).
8. No painel de navegação, selecione Alarmes, Todos os alarmes.

9. Selecione Criar alarme.
10. Selecione o nome da métrica que você criou e, em seguida. escolha Selecionar métrica.
11. Configure o alarme como indicado a seguir e, em seguida, selecione Avançar:
    - Em Estatística, selecione Soma. Isso garante que o número total de pontos de dados do período especificado seja capturado.
    - Em Período, selecione 1 hora.
    - Em Sempre que TimeSinceLastActive for..., escolha Maior que/igual a e insira 10 como limite.
    - Em Additional configuration (Configuração adicional), Datapoints to alarm (Pontos de dados para alarme), deixe o padrão de 1.
12. Escolha Próximo.
13. Em Notification (Notificação), escolha um tópico existente do SNS ou Create new topic (Criar tópico) para criar um. Escolha Próximo.
14. Insira um nome e uma descrição para o alarme e selecione Avançar.
15. Quando terminar de pré-visualizar o alarme, escolha Criar alarme.

Publicar logs de fluxo no Amazon S3

Os logs de fluxo podem publicar dados de log de fluxo no Amazon S3. O Amazon S3 (Simple Storage Service) é um serviço de armazenamento de objetos altamente escalável e durável. Ele foi desenvolvido para armazenar e recuperar qualquer volume de dados, de qualquer lugar na Web. O S3 oferece durabilidade e disponibilidade líderes do setor, além de recursos integrados de controle de versão de dados, criptografia e controle de acesso.

Quando é feita uma publicação no Amazon S3, os dados de log de fluxo são publicados no bucket existente do Amazon S3 especificado. Os registros de log de fluxo para todas as interfaces de rede monitoradas são publicados em uma série de objetos de arquivos de log armazenados no bucket. Se o log de fluxo captura dados para uma VPC, o log de fluxo publica registros de log de fluxo em todas as interfaces de rede da VPC selecionada.

Para criar um bucket do Amazon S3 para usar com logs de fluxo, consulte Criação de um bucket no Guia do usuário do Amazon S3.

Para obter mais informações sobre como simplificar a ingestão de logs de fluxo de VPC, o processamento e a visualização de logs de fluxo, consulte Log centralizado com o OpenSearch na Biblioteca de soluções da AWS.

Para obter mais informações sobre o CloudWatch Logs, consulte Logs enviados ao Amazon S3 no Guia do usuário do Amazon CloudWatch Logs.

Preços

As cobranças de ingestão e de arquivamento de dados para logs vendidos se aplicam quando você publica logs de fluxo no Amazon S3. Para obter mais informações, abra Amazon CloudWatch Pricing (Preços do Amazon CloudWatch), selecione Logs e encontre Vended Logs (Logs fornecidos).

Conteúdo

Arquivos de log de fluxo

O VPC Flow Logs coleta dados sobre o tráfego de IP proveniente de e que segue para a sua VPC em registros de log, agrega esses registros em arquivos de log e publica os arquivos de log no bucket do Amazon S3 em intervalos de 5 minutos. É possível haver a publicação de vários arquivos e cada arquivo de log pode conter alguns ou todos os registros de log de fluxo para o tráfego de IP registrado nos últimos 5 minutos.

No Amazon S3, o campo Last modified (Última modificação) do arquivo de log do fluxo indica a data e hora na qual o arquivo foi carregado para o bucket do Amazon S3. Esta indicação é posterior à data/hora no nome do arquivo e difere pela quantidade de tempo necessária para carregar o arquivo para o bucket do Amazon S3.

Formato do arquivo de log

É possível especificar um dos formatos a seguir para os arquivos de log. Cada arquivo é compactado em um único arquivo Gzip.

- Texto: texto sem formatação. Esse é o formato padrão.
- Parquet: Apache Parquet é um formato colunar de dados. Consultas sobre dados no formato Parquet são 10 a 100 vezes mais rápidas em comparação com consultas em dados em texto

simples. Dados em formato Parquet com compressão Gzip ocupam 20% menos espaço de armazenamento do que o texto simples com compactação Gzip.

> **Note**
>
> Se os dados no formato Parquet com compactação Gzip forem inferiores a 100 KB por período de agregação, o armazenamento de dados no formato Parquet poderá ocupar mais espaço do que texto simples com a compactação Gzip devido aos requisitos de memória do arquivo Parquet.

Opções do arquivo de log

Opcionalmente, é possível especificar as seguintes opções.

- Prefixos S3 compatíveis com Hive: habilite prefixos compatíveis com o Hive em vez de importar partições para as ferramentas compatíveis com o Hive. Antes de executar consultas, use o comando MSCK REPAIR TABLE.
- Partições por hora: se houver um grande volume de logs e tipicamente direcionar consultas para uma hora específica, pode-se obter resultados mais rápidos e economizar em custos de consulta ao particionar os logs a cada hora.

Estrutura do arquivo de log do bucket do S3

Os arquivos de log são salvos no bucket do Amazon S3 especificado por meio de uma estrutura de pastas determinada pelo ID do log de fluxo, pela região, pela data de criação e pelas opções de destino.

Por padrão, os arquivos são entregues no local a seguir.

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/
```

Ao habilitar prefixos S3 compatíveis com HIVE, os arquivos serão entregues no local a seguir.

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/aws-service=vpcflowlogs/
aws-region=region/year=year/month=month/day=day/
```

Ao habilitar partições por hora, os arquivos serão entregues no local a seguir.

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/hour/
```

Ao habilitar partições compatíveis com o Hive e particionar o log de fluxo por hora, os arquivos serão entregues no local a seguir.

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/aws-service=vpcflowlogs/
aws-region=region/year=year/month=month/day=day/hour=hour/
```

Nomes do arquivo de log

O nome de um arquivo de log é baseado na ID do log de fluxo, na região e na data e na hora de criação. Os nomes de arquivo usam o seguinte formato.

```
aws_account_id_vpcflowlogs_region_flow_log_id_YYYYMMDDTHHmmZ_hash.log.gz
```

Veja a seguir um exemplo de arquivo de log para um log de fluxo criado pela conta 123456789012 da AWS para um recurso na região us-east-1 em June 20, 2018 às 16:20 UTC. O arquivo contém os registros de log de fluxo com um horário de término entre 16:20:00 e 16:24:59.

```
123456789012_vpcflowlogs_us-east-1_fl-1234abcd_20180620T1620Z_fe123456.log.gz
```

Permissões do bucket do Amazon S3 para logs de fluxo

Por padrão, os buckets do Amazon S3 e os objetos que eles contêm são privados. Somente o proprietário do bucket pode acessá-los. No entanto, o proprietário do bucket pode conceder acesso a outros recursos e usuários por meio da criação de uma política de acesso.

Se o usuário que cria um log de fluxo for proprietário do bucket e tiver as permissões `PutBucketPolicy` e `GetBucketPolicy` para este bucket, as políticas a seguir serão automaticamente anexadas. Esta política substitui qualquer política existente anexada ao bucket.

Caso contrário, o proprietário do bucket deve adicionar essa política ao bucket, especificando o ID da conta da AWS do criador de log de fluxo ou falha na criação do log de fluxo. Para obter mais informações, consulte Uso de políticas de bucket no Guia do usuário do Amazon Simple Storage Service.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "my-s3-arn/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": account_id,
                    "s3:x-amz-acl": "bucket-owner-full-control"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:account_id:*"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::bucket_name",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": account_id
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:account_id:*"
                }
            }
        }
    ]
}
```

O ARN especificado para *my-s3-arn* depende do uso ou não de prefixos S3 compatíveis com Hive.

- Prefixos padrão

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/account_id/*
```

- Prefixos S3 compatíveis com Hive

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/aws-account-id=account_id/*
```

É uma prática recomendada conceder essas permissões à entidade principal do serviço de entrega de logs em vez de concedê-las a ARNs individuais da Conta da AWS. Outra prática recomendada é o uso das chaves de condição `aws:SourceAccount` e `aws:SourceArn` para se proteger contra O problema do agente confuso. A conta de origem é o proprietário do log de fluxo e o ARN de origem é o ARN curinga (*) do serviço de logs.

Política de chaves obrigatórias para uso com SSE-KMS

É possível proteger os dados no bucket do Amazon S3 habilitando a criptografia no lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) ou a criptografia no lado do servidor com chaves do KMS (SSE-KMS) em seu bucket do S3. Para obter mais informações, consulte Proteger dados usando criptografia do lado do servidor no Manual do usuário do Amazon S3.

Se você escolher SSE-S3, nenhuma configuração adicional será necessária. O Amazon S3 lida com a chave de criptografia.

Se você escolher SSE-KMS, deverá usar um ARN de chave gerenciada pelo cliente. Se você usar um ID de chave, poderá se deparar com um erro LogDestination não pode ser entregue ao criar um log de fluxo. Além disso, você deve atualizar a política de chaves para a chave gerenciada pelo cliente para que a conta de entrega de logs possa gravar no bucket do S3. Para obter mais informações sobre a política de chaves exigida para uso com o SEE-KMS, consulte Criptografia no lado do servidor de buckets do Amazon S3 no Guia do usuário do Amazon CloudWatch Logs.

Permissões de arquivo de log do Amazon S3

Além das políticas de bucket necessárias, o Amazon S3 usa listas de controle de acesso (ACLs) para gerenciar o acesso aos arquivos de log criados por um log de fluxo. Por padrão, o proprietário do bucket tem permissões `FULL_CONTROL` em cada arquivo de log. O proprietário da entrega de logs, se é diferente do proprietário do bucket, não tem nenhuma permissão. A conta de entrega de logs tem permissões `READ` e `WRITE`. Para obter mais informações, consulte Visão geral da lista de controle de acesso (ACL) no Guia do usuário do Amazon S3.

Criar um log de fluxo para publicação no Amazon S3

Depois de criar e configurar o bucket do Amazon S3, você poderá criar logs de fluxo para as interfaces de rede, sub-redes e VPCs.

Pré-requisito

A entidade principal do IAM que cria o log de fluxo deve estar usando um perfil do IAM com as permissões a seguir, necessárias para publicar logs de fluxo no bucket de destino do Amazon S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource": "*"
    }
  ]
}
```

Para criar um log de fluxo usando o console

1. Execute um destes procedimentos:
   - Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/. No painel de navegação, selecione Network Interfaces. Marque a caixa de seleção para a interface de rede.
   - Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/. No painel de navegação, escolha Your VPCs (Suas VPCs). Marque a caixa de seleção da VPC.
   - Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/. No painel de navegação, escolha Sub-redes. Marque a caixa de seleção da sub-rede.
2. Selecione Ações, Criar log de fluxo.
3. Em Filter (Filtro), especifique o tipo de dados de tráfego de IP para registrar em log.
   - Aceitar: registre em log somente o tráfego aceito
   - Rejeitar: registre em log somente o tráfego rejeitado

- Todos: registre em log o tráfego aceito e rejeitado.

4. Em Maximum aggregation interval (Intervalo máximo de agregação), escolha o período máximo durante o qual um fluxo é capturado e agregado em um registro de log de fluxo.
5. Em Destination (Destino), escolha Send to an Amazon S3 bucket (Enviar para um bucket do Amazon S3).
6. Em ARN do bucket do S3, especifique o nome de recurso da Amazon (ARN) de um bucket existente do Amazon S3. Opcionalmente, é possível incluir uma subpasta. Por exemplo, para especificar uma subpasta chamada `my-logs` em um bucket chamado `my-bucket`, use o seguinte ARN:

   ```
   arn:aws:s3:::my-bucket/my-logs/
   ```

   O bucket não pode usar `AWSLogs` como um nome de subpasta, pois se trata de um termo reservado.

   Se você for o proprietário do bucket, uma política de recurso será automaticamernte criada e anexada ao bucket. Para ter mais informações, consulte Permissões do bucket do Amazon S3 para logs de fluxo.
7. Em Formato de registro de log, selecione o formato para o registro de log de fluxo.

   - Para usar o formato de registro de log de fluxo padrão, escolha AWS Formato padrão.
   - Para criar um formato personalizado, escolha Formato personalizado. Em Formato de log, selecione os campos a serem incluídos no registro de log de fluxo.
8. Para Metadados adicionais, escolha se quer incluir metadados do Amazon ECS no formato de log.
9. Em Formato de registro de log, especifique o formato do arquivo de log.

   - Texto: texto sem formatação. Esse é o formato padrão.
   - Parquet: Apache Parquet é um formato colunar de dados. Consultas sobre dados no formato Parquet são 10 a 100 vezes mais rápidas em comparação com consultas em dados em texto simples. Dados em formato Parquet com compressão Gzip ocupam 20% menos espaço de armazenamento do que o texto simples com compactação Gzip.
10. (Opcional) Para usar prefixos S3 compatíveis com o Hive, escolha Prefixo do S3 compatível com Hive, Habilitar.
11. (Opcional) Para particionar seus logs de fluxo por hora, selecione A cada 1 hora (60 minutos).

12. (Opcional) Para adicionar uma etiqueta ao log de fluxo, escolha Adicionar nova tag e especifique a chave e o valor da tag.
13. Selecione Criar log de fluxo.

Como criar um log de fluxo que publique no Amazon S3 usando a linha de comando

Use um dos seguintes comandos:

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

O exemplo de AWS CLI a seguir cria um log de fluxo que captura todo o tráfego da VPC especificada e fornece os logs de fluxo ao bucket do Amazon S3 especificado. O parâmetro `--log-format` especifica um formato personalizado para os registros de log de fluxo.

```
aws ec2 create-flow-logs --resource-type VPC --resource-ids vpc-00112233344556677 --
traffic-type ALL --log-destination-type s3 --log-destination arn:aws:s3:::flow-log-
bucket/custom-flow-logs/ --log-format '${version} ${vpc-id} ${subnet-id} ${instance-
id} ${srcaddr} ${dstaddr} ${srcport} ${dstport} ${protocol} ${tcp-flags} ${type} ${pkt-
srcaddr} ${pkt-dstaddr}'
```

Visualizar registros de log de fluxo com o Amazon S3

Você pode visualizar os registros de log de fluxo usando o console do Amazon S3. Depois que o log de fluxo é criado, pode levar alguns minutos para ele ficar visível no console.

Os arquivos de log são compactados. Quando os arquivos de log são abertos usando o console do Amazon S3, eles serão descompactados, e os registros de log de fluxo serão exibidos. Se os arquivos forem baixados, será necessário descompactá-los para visualizar os registros de log de fluxo.

Como visualizar os registros de log de fluxo publicados no Amazon S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Selecione o nome do bucket para abrir sua página de detalhes.
3. Navegue até a pasta com os arquivos de log. Por exemplo, *prefixo*/AWSLogs/*id_da_conta*/vpcflowlogs/*região*/*ano*/*mês*/*dia*/.
4. Marque a caixa de seleção ao lado do nome do arquivo e escolha Download (Baixar).

Também é possível consultar os registros de log de fluxo nos arquivos de log usando o Amazon Athena. O Amazon Athena é um serviço de consultas interativas que facilita a análise de dados no Amazon S3 usando SQL padrão. Para obter mais informações, consulte Consultar os Amazon VPC Flow Logs no Manual do usuário do Amazon Athena.

Publicar logs de fluxo no Amazon Data Firehose

Os logs de fluxo podem publicar dados de logs de fluxo diretamente no Amazon Data Firehose. O Amazon Data Firehose é um serviço totalmente gerenciado que coleta, transforma e entrega fluxos de dados em tempo real em vários armazenamentos de dados e serviços de analytics da AWS. Ele se encarrega da ingestão de dados em seu nome.

Quando se trata de logs de fluxo de VPC, o Firehose pode ser útil. Os logs de fluxo da VPC capturam informações sobre o tráfego de IP entrando e saindo das interfaces de rede em sua VPC. Esses dados podem ser cruciais para monitoramento de segurança, análise de performance e conformidade regulatória. No entanto, gerenciar o armazenamento e o processamento desse fluxo contínuo de dados de log pode ser uma tarefa complexa e que consome muitos recursos.

Ao integrar o Firehose com seus logs de fluxo de VPC, você pode entregar esses dados ao seu destino preferido, como Amazon S3, Amazon Redshift ou Amazon OpenSearch Service. O Firehose se expandirá para lidar com a ingestão, transformação e entrega de seus logs de fluxo de VPC, aliviando você dessa sobrecarga operacional. Isso permite que você se concentre na análise dos logs e na obtenção de insights, em vez de precisar se preocupar com a infraestrutura subjacente.

Além disso, o Firehose oferece recursos como transformação, compactação e criptografia de dados, os quais podem aumentar a eficiência e a segurança do seu pipeline de processamento de logs de fluxo de VPC. Usar o Firehose para logs de fluxo de VPC pode simplificar o gerenciamento de dados e permitir que você obtenha insights dos dados de tráfego da rede.

Ao publicar no Amazon Data Firehose, os dados de logs de fluxo são publicados em um fluxo de entrega do Amazon Data Firehose como texto sem formatação.

Preços

São aplicadas as taxas padrão de ingestão e entrega. Para obter mais informações, abra Amazon CloudWatch Pricing (Preços do Amazon CloudWatch), selecione Logs e encontre Vended Logs (Logs fornecidos).

Conteúdo

- Perfis do IAM para entrega entre contas
- Criar um log de fluxo para publicação no Amazon Data Firehose

Perfis do IAM para entrega entre contas

Ao publicar no Amazon Data Firehose, você pode escolher um fluxo de entrega que esteja na mesma conta que o recurso a ser monitorado (a conta de origem) ou em uma conta diferente (a conta de destino). Para permitir a entrega de logs de fluxo entre contas para o Amazon Data Firehose, você deve criar um perfil do IAM na conta de origem e um perfil do IAM na conta de destino.

Perfis

- Função da conta de origem
- Função da conta de destino

Função da conta de origem

Na conta de origem, crie uma função que conceda as seguintes permissões. Neste exemplo, o nome do perfil é `mySourceRole`, mas é possível escolher um nome diferente para este perfil. A última instrução permite que o perfil na conta de destino assuma este perfil. As instruções de condição garantem que esse perfil seja passado somente para o serviço de entrega de logs e somente ao monitorar o recurso especificado. Ao criar a política, especifique as VPCs, as interfaces de rede ou as sub-redes que sendo monitoradas com a chave de condição `iam:AssociatedResourceARN`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::source-account:role/mySourceRole",
      "Condition": {
          "StringEquals": {
              "iam:PassedToService": "delivery.logs.amazonaws.com"
          },
          "StringLike": {
              "iam:AssociatedResourceARN": [
                  "arn:aws:ec2:region:source-account:vpc/vpc-00112233344556677"
              ]
```

```
            }
        }
    },
    {
      "Effect": "Allow",
      "Action": [
          "logs:CreateLogDelivery",
          "logs:DeleteLogDelivery",
          "logs:ListLogDeliveries",
          "logs:GetLogDelivery"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole"
    }
  ]
}
```

Verifique se a essa função tem a política de confiança a seguir, que permite que o serviço de entrega de logs assuma a função.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Na conta de origem, use o procedimento a seguir para criar a função.

Para criar a função da conta de origem

1. Abra o console do IAM, em https://console.aws.amazon.com/iam/.

2. No painel de navegação, escolha Policies.
3. Selecione Criar política.
4. Na página Create policy (Criar política) faça o seguinte:
   a. Escolha JSON.
   b. Substitua o conteúdo dessa janela pela política de permissões no início desta seção.
   c. Escolha Próximo.
   d. Insira um nome e uma descrição e tags opcionais para a política e escolha Criar política.
5. No painel de navegação, selecione Perfis.
6. Escolha Criar Perfil.
7. Em Trusted entity type (Tipo de entidade confiável), escolha Custom trust policy (Política de confiança personalizada). Em Custom trust policy (Política de confiança personalizada), substitua `"Principal": {},` pelo seguinte, que especifica o serviço de entrega de logs. Selecione Avançar.

```
"Principal": {
   "Service": "delivery.logs.amazonaws.com"
},
```

8. Na página Adicionar permissões, marque a caixa de seleção correspondente à política criada anteriormente neste procedimento e, em seguida, escolha Avançar.
9. Insira um nome para a função e, opcionalmente, uma descrição.
10. Selecione Criar perfil.

Função da conta de destino

Na conta de destino, crie uma função com um nome que comece com AWSLogDeliveryFirehoseCrossAccountRole. Esse perfil deve conceder as seguintes permissões.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
          "iam:CreateServiceLinkedRole",
          "firehose:TagDeliveryStream"
```

```
      ],
      "Resource": "*"
    }
  ]
}
```

Certifique-se de que essa função tenha a seguinte política de confiança, que permite que a função que você criou na conta de origem assuma esta função.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::source-account:role/mySourceRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Na conta de destino, use o procedimento a seguir para criar a função.

Para criar a função da conta de destino

1. Abra o console do IAM, em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Policies.
3. Selecione Criar política.
4. Na página Create policy (Criar política) faça o seguinte:
   a. Escolha JSON.
   b. Substitua o conteúdo dessa janela pela política de permissões no início desta seção.
   c. Escolha Próximo.
   d. Insira um nome para a política que comece com AWSLogDeliveryFirehoseCrossAccountRole e, em seguida, selecione Criar política.
5. No painel de navegação, selecione Perfis.
6. Escolha Criar Perfil.

7. Em Trusted entity type (Tipo de entidade confiável), escolha Custom trust policy (Política de confiança personalizada). Em Custom trust policy (Política de confiança personalizada), substitua `"Principal": {},` pelo seguinte, que especifica a função da conta de origem. Escolha Próximo.

```
"Principal": {
   "AWS": "arn:aws:iam::source-account:role/mySourceRole"
},
```

8. Na página Adicionar permissões, marque a caixa de seleção correspondente à política criada anteriormente neste procedimento e, em seguida, escolha Avançar.
9. Insira um nome para a função e, opcionalmente, uma descrição.
10. Selecione Criar perfil.

Criar um log de fluxo para publicação no Amazon Data Firehose

É possível criar logs de fluxos para suas VPCs, sub-redes ou interfaces de rede.

Pré-requisitos

- Crie o fluxo de entrega de destino do Amazon Data Firehose. Usar Direct Put (Inserção direta) como origem. Para obter mais informações, consulte Criar um fluxo de entrega do Amazon Data Firehose.
- Se você estiver publicando logs de fluxo em uma conta diferente, crie os perfis do IAM necessários, conforme descrito em the section called “Perfis do IAM para entrega entre contas”.

Para criar um log de fluxo que publique no Amazon Data Firehose

1. Execute um destes procedimentos:
   - Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/. No painel de navegação, selecione Network Interfaces. Marque a caixa de seleção para a interface de rede.
   - Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/. No painel de navegação, escolha Your VPCs (Suas VPCs). Marque a caixa de seleção da VPC.
   - Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/. No painel de navegação, escolha Sub-redes. Marque a caixa de seleção da sub-rede.
2. Selecione Ações, Criar log de fluxo.

3. Em Filter (Filtrar), especifique o tipo de tráfego a ser registrado em log.
   - Accept (Aceitar): registre em log somente o tráfego aceito
   - Reject (Rejeitar): registre em log somente o tráfego rejeitado
   - All (Todos): registre em log o tráfego aceito e rejeitado
4. Em Maximum aggregation interval (Intervalo máximo de agregação), escolha o período máximo durante o qual um fluxo é capturado e agregado em um registro de log de fluxo.
5. Em Destination (Destino), escolha uma das seguintes opções:
   - Enviar para o Amazon Data Firehose na mesma conta: o fluxo de entrega e o recurso a serem monitorados estão na mesma conta.
   - Enviar para o Amazon Data Firehose em uma conta diferente: o fluxo de entrega e o recurso a serem monitorados estão em contas diferentes.
6. No nome do fluxo do Amazon Data Firehose, selecione o fluxo de entrega que você criou.
7. [Somente para entrega entre contas] Para o Acesso ao serviço, escolha um perfil de serviço do IAM existente para entrega entre contas que tenha permissões para publicar logs ou selecione Configurar permissões para abrir o console do IAM e criar um perfil de serviço.
8. Em Formato de registro de log, selecione o formato para o registro de log de fluxo.
   - Para usar o formato de registro de log de fluxo padrão, escolha AWS Formato padrão.
   - Para criar um formato personalizado, escolha Formato personalizado. Em Formato de log, selecione os campos a serem incluídos no registro de log de fluxo.
9. Para Metadados adicionais, escolha se quer incluir metadados do Amazon ECS no formato de log.
10. (Opcional) Escolha Adicionar tag para aplicar tags ao log de fluxo.
11. Selecione Criar log de fluxo.

Como criar um log de fluxo que publique no Amazon Data Firehose usando a linha de comando

Use um dos seguintes comandos:

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

O exemplo de AWS CLI a seguir cria um log de fluxo que captura todo o tráfego da VPC especificada e entrega os logs de fluxo ao fluxo de entrega do Amazon Data Firehose na mesma conta.

```
aws ec2 create-flow-logs --traffic-type ALL \
  --resource-type VPC \
  --resource-ids vpc-00112233344556677 \
  --log-destination-type kinesis-data-firehose \
  --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream/flowlogs_stream
```

O exemplo de AWS CLI a seguir cria um log de fluxo que captura todo o tráfego da VPC especificada e entrega os logs de fluxo ao fluxo de entrega do Amazon Data Firehose em uma conta diferente.

```
aws ec2 create-flow-logs --traffic-type ALL \
  --resource-type VPC \
  --resource-ids vpc-00112233344556677 \
  --log-destination-type kinesis-data-firehose \
  --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream/flowlogs_stream \
  --deliver-logs-permission-arn arn:aws:iam::source-account:role/mySourceRole \
  --deliver-cross-account-role arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole
```

Como resultado da criação do log de fluxo, é possível obter os dados de log de fluxo no destino que você configurou para o fluxo de entrega.

Consultar logs de fluxo usando o Amazon Athena

O Amazon Athena é um serviço de consulta interativa que permite analisar dados no Amazon S3, como seus logs de fluxo, usando o SQL padrão. Você pode usar o Athena com o VPC Flow Logs para obter rapidamente insights acionáveis sobre o tráfego que atravessa a sua VPC. Por exemplo, você pode identificar quais recursos em suas virtual private clouds (VPCs) são os principais locutores ou identificar os endereços IP com as conexões TCP mais rejeitadas.

Opções

- Você pode simplificar e automatizar a integração dos logs de fluxo da VPC com o Athena gerando um modelo do CloudFormation que cria os recursos necessários da AWS e as consultas predefinidas que você pode executar para obter insights sobre o tráfego que atravessa a VPC.

- Você pode criar suas próprias consultas usando o Athena. Para obter mais informações, consulte Consulta de logs de fluxo usando o Amazon Athena no Guia do usuário do Amazon Athena.

Preços

Você incorre em cobranças padrão do Amazon Athena pelas consultas feitas. Cobranças padrão da AWS Lambda serão aplicadas à função do Lambda que carrega novas partições em uma programação recorrente (para quando você especifica uma frequência de carregamento de partição, mas deixa de especificar uma data de início e término).

Para usar as consultas predefinidas

- Gerar o modelo do CloudFormation usando o console
- Gerar o modelo do CloudFormation usando a AWS CLI
- Executar uma consulta predefinida

Gerar o modelo do CloudFormation usando o console

Depois que os primeiros logs de fluxo forem entregues ao seu bucket do S3, você pode integrar ao Athena gerando um modelo do CloudFormation e usando o modelo para criar uma pilha.

Requisitos

- A região selecionada deve ser compatível com o AWS Lambda e o Amazon Athena.
- Os buckets do Amazon S3 devem estar na região selecionada.
- O formato de registro de log para o log de fluxo deve incluir os campos usados pelas consultas predefinidas específicas que você desejar executar.

Para gerar o modelo usando o console

1. Execute um destes procedimentos:
   - Abra o console da Amazon VPC. No painel de navegação, escolha Your VPCs (Suas VPCs) e, em seguida, selecione a sua VPC.
   - Abra o console da Amazon VPC. No painel de navegação, escolha Subnets (Sub-redes) e, em seguida, selecione a sua sub-rede.
   - Abra o console do Amazon EC2. No painel de navegação, escolha Network Interfaces (Interfaces de rede) e, em seguida, selecione a sua interface de rede.

2. Na guia Flow logs (Logs de fluxo), selecione um log de fluxo que publica no Amazon S3 e, em seguida, escolha Actions (Ações) e Generate Athena integration (Gerar integração ao Athena).
3. Especifique a frequência de carregamento da partição. Se escolher None (Nenhum), você deve especificar as datas de início e término da partição, usando datas do passado. Se escolher Daily (Diário), Weekly (Semanal) ou Monthly (Mensal), as datas de início e término da partição serão opcionais. Se você não especificar datas de início e término, o modelo do CloudFormation cria uma função do Lambda que carrega novas partições em uma programação recorrente.
4. Selecione ou crie um bucket do S3 para o modelo gerado e um bucket do S3 para os resultados da consulta.
5. Escolha Generate Athena integration (Gerar integração ao Athena).
6. (Opcional) Na mensagem de êxito, escolha o link para navegar até o bucket que especificou para o modelo do CloudFormation e personalize o modelo.
7. Na mensagem de êxito, escolha Create CloudFormation stack (Criar pilha do CloudFormation) para abrir o assistente Create Stack (Criar pilha) no console do AWS CloudFormation. A URL do modelo do CloudFormation gerado é especificado na seção Template (Modelo). Conclua o assistente para criar os recursos especificados no modelo.

Recursos desenvolvidos pelo modelo do CloudFormation

- Um banco de dados do Athena. O nome do banco de dados é vpcflowlogsathenadatabase<flow-logs-subscription-id>.
- Um grupo de trabalho do Athena. O nome do grupo de trabalho é <flow-log-subscription-id><partition-load-frequency><start-date><end-date>workgroup
- Uma tabela particionada do Athena que corresponde aos seus registros de log de fluxo. O nome da tabela é <flow-log-subscription-id><partition-load-frequency><start-date><end-date>.
- Um conjunto de consultas nomeadas do Athena. Para obter mais informações, consulte Consultas predefinidas.
- Uma função do Lambda que carrega novas partições para a tabela de acordo com a programação especificada (diária, semanal ou mensal).
- Uma função do IAM que concede permissão para executar as funções do Lambda.

Gerar o modelo do CloudFormation usando a AWS CLI

Depois que os primeiros logs de fluxo forem entregues ao bucket do S3, você poderá gerar e usar um modelo do CloudFormation para fazer a integração ao Athena.

Use o comando a seguir get-flow-logs-integration-template para gerar o modelo do CloudFormation.

```
aws ec2 get-flow-logs-integration-template --cli-input-json file://config.json
```

Este é um exemplo do arquivo `config.json`.

```
{
    "FlowLogId": "fl-12345678901234567",
    "ConfigDeliveryS3DestinationArn": "arn:aws:s3:::my-flow-logs-athena-integration/
templates/",
    "IntegrateServices": {
        "AthenaIntegrations": [
            {
                "IntegrationResultS3DestinationArn": "arn:aws:s3:::my-flow-logs-
analysis/athena-query-results/",
                "PartitionLoadFrequency": "monthly",
                "PartitionStartDate": "2021-01-01T00:00:00",
                "PartitionEndDate": "2021-12-31T00:00:00"
            }
        ]
    }
}
```

Use o comando a seguir create-stack para criar uma pilha usando o modelo do CloudFormation gerado.

```
aws cloudformation create-stack --stack-name my-vpc-flow-logs --template-body file://
my-cloudformation-template.json
```

Executar uma consulta predefinida

O modelo do CloudFormation gerado fornece um conjunto de consultas predefinidas que você pode realizar para obter rapidamente insights significativos sobre o tráfego em sua rede da AWS. Depois de criar a pilha e verificar se todos os recursos foram criados corretamente, você pode realizar uma das consultas predefinidas.

Para realizar uma consulta predefinida usando o console

1. Abra o console do Athena.
2. No painel de navegação, selecione Query editor (Editor de consultas). Em Workgroup (Grupo de trabalho), selecione o grupo de trabalho criado pelo modelo do CloudFormation.
3. Selecione Saved queries (Consultas salvas), selecione uma consulta, modifique os parâmetros conforme necessário e execute a consulta. Para obter uma lista das consultas predefinidas disponíveis, consulte Predefined queries (Consultas predefinidas).
4. Em Query results (Resultados da consulta), veja os resultados da consulta.

Consultas predefinidas

A seguir, uma lista completa das consultas nomeadas do Athena. As consultas predefinidas fornecidas quando você gera o modelo dependem dos campos que fazem parte do formato de registro de log para o log de fluxo. Assim sendo, o modelo pode não conter todas essas consultas predefinidas.

- VPCFlowLogsAcceptedTraffic: as conexões TCP que foram permitidas com base nos seus grupos de segurança e ACLs de rede.
- VpcFlowLogsAdminPortTraffic: os 10 principais endereços IP com mais tráfego, conforme registrado por aplicações que atendem solicitações em portas administrativas.
- VPCFlowLogsiPv4Traffic: o total registrado de bytes de tráfego IPv4.
- VPCFlowLogsiPv6Traffic: o total registrado de bytes de tráfego IPv6.
- VPCFlowLogsRejectedTCPTraffic: as conexões TCP que foram rejeitadas com base nos seus grupos de segurança ou ACLs de rede.
- VPCFlowLogsRejectedTraffic: o tráfego que foi rejeitado com base nos seus grupos de segurança ou ACLs de rede.
- VPCFlowLogsShrdpTraffic: o tráfego SSH e RDP.
- VPCFlowLogStopTalkers: os 50 endereços IP com mais tráfego registrado.
- VPCFlowLogStopTalkersPacketLevel: os 50 endereços IP no nível de pacote com mais tráfego registrado.
- VPCFlowLogStoptalkingInstances: os IDs das 50 instâncias com mais tráfego registrado.
- VPCFlowLogStopTalkingSubnets: os IDs das 50 sub-redes com mais tráfego registrado.
- VPCFlowLogStoptCPTraffic: todo o tráfego TCP registrado para um endereço IP de origem.

- VPCFlowLogsTotalByTestransFerred: os 50 pares de endereços IP de origem e destino com mais bytes registrados.
- VPCFlowLogsTotalByTestRansFerredPacketLevel: os 50 pares de endereços IP de origem e destino no nível de pacote com mais bytes registrados.
- VPCFlowLogsTrafficFrmsRcaddr: o tráfego registrado para um endereço IP de origem específico.
- VPCFlowLogsTrafficTodStaddr: o tráfego registrado para um endereço IP de destino específico.

Solucionar problemas do VPC Flow Logs

Veja a seguir os possíveis problemas que você pode ter ao trabalhar com logs de fluxo.

Problemas

- Registros incompletos de log de fluxo
- O log de fluxo está ativo, mas não há registro de log de fluxo nem grupo de logs
- Erro “LogDestinationNotFoundException” ou “Access Denied for LogDestination”
- Exceder o limite de políticas de buckets do Amazon S3
- LogDestination não pode ser entregue

Registros incompletos de log de fluxo

Problema

Os registros do log de fluxo estão incompletos ou não estão mais sendo publicados.

Causa

Pode haver um problema ao entregar os logs de fluxo para o grupo de logs do CloudWatch Logs.

Solução

Tanto no console do Amazon EC2 quanto no console da Amazon VPC, selecione a guia Flow Logs (Logs de fluxo) do recurso em questão. A tabela de logs de fluxo exibe qualquer erro na coluna Status. Outra opção é usar o comando describe-flow-logs e verificar o valor retornado no campo `DeliverLogsErrorMessage`. Um dos erros a seguir pode ser exibido:

- `Rate limited`: esse erro poderá ocorrer se o controle de utilização de logs do CloudWatch Logs tiver sido aplicado: quando o número de registros de log de fluxo de uma interface de rede for

superior ao número máximo de registros que podem ser publicados em um intervalo de tempo específico. Esse erro também poderá ocorrer se for atingida a cota do número de grupos de logs do CloudWatch Logs que podem ser criados. Para obter mais informações, consulte cotas de serviço do CloudWatch no Manual do usuário do Amazon CloudWatch.

- `Access error`: esse erro pode ocorrer por um dos seguintes motivos:
  - A função do IAM de seu log de fluxo não tem permissões suficientes para publicar registros de log de fluxo no grupo de logs do CloudWatch.
  - A função do IAM não tem uma relação de confiança com o serviço de logs de fluxo
  - A relação de confiança não especifica o serviço de logs de fluxo como principal

  Para ter mais informações, consulte Perfil do IAM para publicar logs de fluxo no CloudWatch Logs.
- `Unknown error`: ocorreu um erro interno nos logs de fluxos.

O log de fluxo está ativo, mas não há registro de log de fluxo nem grupo de logs

Problema

Você criou um log de fluxo. O console da Amazon VPC ou do Amazon EC2 exibe esse log de fluxo como `Active`. No entanto, não é possível ver nenhum stream de log no CloudWatch Logs nem arquivos de log no bucket do Amazon S3.

Possíveis causas

- O log de fluxo ainda está sendo criado. Em alguns casos, pode demorar dez minutos ou mais após a criação do log de fluxo para que o grupo de logs seja criado e para que os dados sejam exibidos.
- Nenhum tráfego foi registrado até o momento para suas interfaces de rede. O grupo de logs no CloudWatch Logs só é criado quando o tráfego é registrado.

Solução

Aguarde alguns minutos para que o grupo de logs seja criado ou para o tráfego ser registrado.

Erro “LogDestinationNotFoundException” ou “Access Denied for LogDestination”

Problema

Você recebe um erro `Access Denied for LogDestination` ou `LogDestinationNotFoundException` quando tenta criar um log de fluxo.

Possíveis causas

- Ao criar um log de fluxo que publica dados em um bucket do Amazon S3, esse erro indica que o bucket do S3 especificado não pôde ser encontrado ou que a política de bucket não permite que logs sejam entregues ao bucket.
- Ao criar um log de fluxo que publica dados no Amazon CloudWatch Logs, esse erro indica que a função do IAM não permite que os logs sejam entregues ao grupo de logs.

Solução

- Ao publicar no Amazon S3, verifique se você especificou o ARN de um bucket do S3 existente e se o ARN está no formato correto. Se não for proprietário do bucket do S3, verifique se a política de bucket tem as permissões necessárias e usa o ID da conta e o nome do bucket corretos no ARN.
- Ao publicar no CloudWatch Logs, verifique se a função do IAM tem as permissões necessárias.

Exceder o limite de políticas de buckets do Amazon S3

Problema

Você obtém o seguinte erro ao tentar criar um log de fluxo: `LogDestinationPermissionIssueException`.

Possíveis causas

As políticas de buckets do Amazon S3 são limitadas a 20 KB.

Toda vez que você cria um log de fluxo que é publicado em um bucket do Amazon S3, automaticamente adicionamos o ARN do bucket especificado, que inclui o caminho da pasta, ao elemento `Resource` na política do bucket.

Criar vários logs de fluxo que são publicados no mesmo bucket pode fazer com que você exceda o limite da política do bucket.

Solução

- Limpe a política de bucket removendo as entradas de log de fluxo que não são mais necessárias.
- Conceda permissões para o bucket inteiro substituindo as entradas de log de fluxo individuais pelo seguinte.

```
arn:aws:s3:::bucket_name/*
```

Se você conceder permissões para o bucket inteiro, as novas assinaturas de log de fluxo não adicionam novas permissões à política de bucket.

LogDestination não pode ser entregue

Problema

Você obtém o seguinte erro ao tentar criar um log de fluxo: `LogDestination <bucket name> is undeliverable`.

Possíveis causas

O bucket de destino do Amazon S3 é criptografado usando a criptografia do lado do servidor com AWS KMS (SSE-KMS) e a criptografia padrão do bucket é um ID de chave do KMS.

Solução

O valor deve ser um ARN de chave do KMS. Altere o tipo de criptografia S3 padrão, de ID da chave KMS para ARN de chave do KMS. Para obter mais informações, consulte Configuração da criptografia padrão no Guia do usuário do Amazon Simple Storage Service.

Métricas do CloudWatch para suas VPCs

A Amazon VPC publica dados sobre suas VPCs no Amazon CloudWatch. Você pode recuperar estatísticas sobre suas VPCs como um conjunto ordenado de dados de séries temporais, conhecidos como métricas. Considere uma métrica como uma variável a ser monitorada, e os dados como o valor dessa variável ao longo do tempo. Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch.

Conteúdo

- Métricas e dimensões do NAU
- Habilitar ou desabilitar o monitoramento do NAU
- Exemplo de alarmes do NAU do CloudWatch

Métricas e dimensões do NAU

O Uso de endereço de rede (NAU) é uma métrica aplicada aos recursos da sua rede virtual para ajudar você a planejar e monitorar o tamanho da sua VPC. Não há custo para monitorar o NAU. O monitoramento do NAU é útil porque, se você esgotar o NAU ou as cotas do NAU emparelhadas para sua VPC, não poderá iniciar novas instâncias do EC2 nem provisionar novos recursos, como endpoints da VPC do Network Load Balancers, funções do Lambda, anexos do gateway de trânsito ou gateways NAT.

Se você tiver habilitado o monitoramento do Uso de endereço de rede (NAU, Network Address Usage) para uma VPC, a Amazon VPC enviará métricas relacionadas ao NAU ao Amazon CloudWatch. O tamanho de uma VPC é medido pelo número de unidades de uso de endereço de rede (NAU) que a VPC contém.

Você pode usar essas métricas para entender a taxa de crescimento da sua VPC, prever quando sua VPC atingirá o limite de tamanho ou criar alarmes quando os limites de tamanho forem ultrapassados.

O namespace `AWS/EC2` inclui as seguintes métricas para o monitoramento do NAU.

Métrica	Descrição
`NetworkAddressUsage`	A contagem de NAU por VPC. Critérios de relatórios • A cada 24 horas. Dimensões • Nome: `Per-VPC Metrics`, Valor: o ID da VPC.
`NetworkAddressUsagePeered`	A contagem do NAU para a VPC e todas as VPCs com as quais ela está emparelhada. Critérios de relatórios • A cada 24 horas.

Métrica	Descrição
	Dimensões • Nome: `Per-VPC Metrics`, Valor: o ID da VPC.

O namespace `AWS/Usage` inclui as seguintes métricas para o monitoramento do NAU.

Métrica	Descrição
`ResourceCount`	A contagem de NAU por VPC. Critérios de relatórios • A cada 24 horas. Dimensões • Nome: `Service`, Valor: `EC2` • Nome: `Type`, Valor: `Resource` • Nome: `Resource`, Valor: o ID da VPC. • Nome: `Class`, Valor: `NetworkAddressUsage`
`ResourceCount`	A contagem do NAU para a VPC e todas as VPCs com as quais ela está emparelhada. Critérios de relatórios • A cada 24 horas. Dimensões • Nome: `Service`, Valor: `EC2` • Nome: `Type`, Valor: `Resource` • Nome: `Resource`, Valor: o ID da VPC.

Métrica	Descrição
	• Nome: `Class`, Valor: `NetworkAddressUsagePeered`
`ResourceCount`	Uma visão combinada do uso do NAU nas VPCs. Critérios de relatórios • A cada 24 horas. Dimensões • Nome: `Service`, Valor: `EC2` • Nome: `Type`, Valor: `Resource` • Nome: `Resource`, Valor: `VPC` • Nome: `Class`, Valor: `NetworkAddressUsage`
`ResourceCount`	Uma visão combinada do uso do NAU nas VPCs emparelhadas. Critérios de relatórios • A cada 24 horas. Dimensões • Nome: `Service`, Valor: `EC2` • Nome: `Type`, Valor: `Resource` • Nome: `Resource`, Valor: `VPC` • Nome: `Class`, Valor: `NetworkAddressUsagePeered`

Habilitar ou desabilitar o monitoramento do NAU

Para visualizar as métricas do NAU no CloudWatch, primeiro você deve habilitar o monitoramento em cada VPC para monitorar.

Para habilitar ou desabilitar o monitoramento do NAU

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Marque a caixa de seleção da VPC.
4. Selecione Actions (Ações), Edit VPC settings (Editar configurações da VPC).
5. Execute um destes procedimentos:
   - Para habilitar o monitoramento, selecione Network mapping units metrics settings (Configurações das métricas das unidades de mapeamento de rede), Enable network address usage metrics (Habilitar métricas de uso de endereço de rede).
   - Para desabilitar o monitoramento, desmarque Network mapping units metrics settings (Configurações das métricas das unidades de mapeamento de rede), Enable network address usage metrics (Habilitar métricas de uso de endereço de rede).

Para habilitar ou desabilitar o monitoramento usando a linha de comando

- modify-vpc-attribute (AWS CLI)
- Edit-EC2VpcAttribute (AWS Tools for Windows PowerShell)

Exemplo de alarmes do NAU do CloudWatch

É possível usar o comando da AWS CLI e o `.json` de exemplo a seguir para criar um alarme do Amazon CloudWatch e uma notificação do SNS para rastrear a utilização de NAU da VPC usando 50.000 NAUS como limiar. Este exemplo exige que você primeiro crie um tópico do Amazon SNS. Para obter mais informações, consulte Conceitos básicos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service.

```
aws cloudwatch put-metric-alarm --cli-input-json file://nau-alarm.json
```

Veja a seguir um exemplo de `nau-alarm.json`.

```
{
    "Namespace": "AWS/EC2",
    "MetricName": "NetworkAddressUsage",
    "Dimensions": [{
        "Name": "Per-VPC Metrics",
        "Value": "vpc-0123456798"
    }],
    "AlarmActions": ["arn:aws:sns:us-west-1:123456789012:my_sns_topic"],
    "ComparisonOperator": "GreaterThanThreshold",
    "Period": 86400,
    "EvaluationPeriods": 1,
    "Threshold": 50000,
    "AlarmDescription": "Tracks NAU utilization of the VPC with 50k NAUs as the
 threshold",
    "AlarmName": "VPC NAU Utilization",
    "Statistic": "Maximum"
}
```

Gerenciar responsabilidades pela segurança na Amazon Virtual Private Cloud

A segurança da nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você contará com um data center e uma arquitetura de rede criados para atender aos requisitos das organizações com as maiores exigências de segurança.

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

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa serviços AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados com segurança. Auditores terceirizados testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam à Amazon Virtual Private Cloud, consulte Serviços da AWS no escopo por programa de conformidade.
- Segurança na nuvem: sua responsabilidade é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar a Amazon VPC. Os tópicos a seguir mostram como configurar a Amazon VPC para atender aos seus objetivos de segurança e de conformidade. Você também aprenderá a usar outros serviços da AWS que ajudam a monitorar e proteger os recursos da Amazon VPC.

Conteúdo

- Melhores práticas de segurança para a VPC

Garantir a proteção de dados na Amazon Virtual Private Cloud

O modelo de responsabilidade compartilhada da AWS se aplica à proteção de dados na Amazon Virtual Private Cloud. Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Data Privacy FAQ. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and RGPD no Blog de segurança da AWS.

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

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos da AWS. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure os logs de API e atividade do usuário com AWS CloudTrail. Para obter informações sobre como usar as trilhas do CloudTrail para capturar atividades da AWS, consulte Working with CloudTrail trails no Guia do usuário do AWS CloudTrail.
- Use as soluções de criptografia AWS, juntamente com todos os controles de segurança padrão em Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar a AWS por meio de uma interface de linha de comandos ou de uma API, use um endpoint do FIPS. Para obter mais informações sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sigilosas, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso

também vale para o uso do Amazon VPC ou de outros Serviços da AWS com o console, a API, a AWS CLI ou os AWS SDKs. Quaisquer dados inseridos em tags ou em campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

Garantir a privacidade do tráfego entre redes na Amazon VPC

A Amazon Virtual Private Cloud oferece recursos que podem ser usados para ampliar e monitorar a proteção da Virtual Private Cloud (VPC):

- Grupos de segurança: os grupos de segurança permitem determinado tráfego de entrada e saída no nível do recurso (como uma instância do EC2). Quando você inicia uma instância, atribui a ela um ou mais grupos de segurança. Cada instância na VPC pode pertencer a um conjunto diferente de grupos de segurança. Se você não especificar um grupo de segurança ao iniciar uma instância, ela será associada automaticamente ao grupo de segurança padrão da VPC. Para ter mais informações, consulte Grupos de segurança.
- Listas de controle de acesso (ACL) à rede: as ACLs da rede permitem ou negam determinado tráfego de entrada e de saída no nível da sub-rede. Para ter mais informações, consulte Controlar o tráfego da sub-rede com listas de controle de acesso à rede.
- Logs de fluxos: os logs de fluxos capturam informações sobre o tráfego de IP de e para as interfaces de rede em sua VPC. É possível criar um log de fluxos para uma VPC, sub-rede ou interface de rede. Os dados de log de fluxo são publicados no CloudWatch Logs ou no Amazon S3 e podem ajudar a diagnosticar regras de ACL de rede e grupos de segurança excessivamente restritivos ou permissivos. Para obter mais informações, consulte Como registrar tráfego IP em log com logs de fluxo da VPC.
- Espelhamento de tráfego: é possível copiar o tráfego de rede de uma interface de rede elástica de uma instância do Amazon EC2. Depois, é possível enviar o tráfego para dispositivos de monitoramento e segurança fora de banda. Para obter mais informações, consulte o Guia de espelhamento de tráfego.

Identity and Access Management para o Amazon VPC

O AWS Identity and Access Management (IAM) é um serviço da AWS service (Serviço da AWS) que ajuda um administrador a controlar com segurança o acesso aos recursos da AWS. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (ter

permissões) para usar os recursos da Amazon VPC. O IAM é um AWS service (Serviço da AWS) que pode ser usado sem custo adicional.

Conteúdo

Público

A forma de usar o AWS Identity and Access Management (IAM) varia em função do trabalho realizado na Amazon VPC.

Usuário do serviço: se você usar o serviço do Amazon VPC para fazer seu trabalho, o administrador fornecerá as credenciais e as permissões necessárias. À medida que mais recursos do Amazon VPC forem usados para realizar o trabalho, talvez sejam necessárias permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não puder acessar um recurso na Amazon VPC, consulte Solução de problemas de identidade e acesso da Amazon VPC.

Administrador do serviço: se você for o responsável pelos recursos da Amazon VPC em sua empresa, você provavelmente terá acesso total à Amazon VPC. É seu trabalho determinar quais recursos da Amazon VPC os funcionários devem acessar. Envie solicitações ao administrador do IAM para alterar as permissões dos usuários do serviço. Revise as informações nesta página para entender os conceitos básicos do IAM. Para saber mais sobre como a empresa pode usar o IAM com a Amazon VPC, consulte Como a Amazon VPC funciona com o IAM.

Administrador do IAM: se você é um administrador do IAM, talvez queira saber detalhes sobre como pode escrever políticas para gerenciar o acesso à Amazon VPC. Para ver exemplos de políticas, consulte Exemplos de políticas da Amazon VPC.

Autenticar com identidades

A autenticação é a forma como fazer login na AWS usando suas credenciais de identidade. É necessário ser autenticado (fazer login na AWS) como Usuário raiz da conta da AWS, como usuário do IAM, ou assumindo um perfil do IAM.

É possível fazer login na AWS como uma identidade federada usando credenciais fornecidas por uma fonte de identidades. AWS IAM Identity Center (Centro de Identidade do IAM), a autenticação única da empresa e as suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Quando você acessa a AWS usando a federação, está indiretamente assumindo um perfil.

A depender do tipo de usuário, você pode fazer login no AWS Management Console ou no portal de acesso AWS. Para obter mais informações sobre como fazer login na AWS, consulte Como fazer login na contaConta da AWS no Início de Sessão da AWS Guia do usuário.

Se você acessar a AWS de forma programática, a AWS fornecerá um kit de desenvolvimento de software (SDK) e uma interface de linha de comandos (CLI) para você assinar de forma criptográfica as solicitações usando as suas credenciais. Se você não utilizar as ferramentas da AWS, deverá assinar as solicitações por conta própria. Para obter mais informações sobre como usar o método recomendado para designar solicitações por conta própria, consulte Versão 4 do AWS Signature para solicitações de API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser necessário fornecer informações adicionais de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais, consulte Autenticação multifator no Guia do usuário do AWS IAM Identity Center e Usar a autenticação multifator da AWS no IAM no Guia do usuário do IAM.

Usuário-raiz Conta da AWS

Ao criar uma Conta da AWS, você começa com uma identidade de login com acesso completo a todos os Serviços da AWS e recursos na conta. Essa identidade, chamada usuário-raiz da Conta da AWS, é acessada por login com o endereço de e-mail e a senha usada para criar a conta. É altamente recomendável não usar o usuário-raiz para tarefas diárias. Proteja as credenciais do usuário-raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário-raiz, consulte Tarefas que exigem credenciais de usuário-raiz no Guia do Usuário do IAM.

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas para uma única pessoa ou aplicação. Sempre que possível, é recomendável contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, é recomendável alternar as chaves de acesso. Para obter mais informações, consulte Alternar as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Casos de uso para usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Um perfil do IAM é uma identidade na Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Para assumir temporariamente um perfil do IAM no AWS Management Console, você pode alternar de um usuário para um perfil do IAM (console). É possível presumir um perfil chamando uma operação de API da AWS CLI ou da AWS, ou usando um URL personalizado. Para obter mais informações sobre métodos para usar perfis, consulte Métodos para assumir um perfil no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, é possível criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas por ele. Para ter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidade de terceiros (federação) no Guia do usuário do IAM. Se usar o Centro de Identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de Identidade do IAM correlaciona o conjunto de permissões a

um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Guia do Usuário do AWS IAM Identity Center.

- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, alguns Serviços da AWS permitem anexar uma política diretamente a um recurso (em vez de usar um perfil como proxy). Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.
- Acesso entre serviços: alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal da chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
  - Sessões de acesso direto (FAS): qualquer pessoa que utilizar um perfil ou usuário do IAM para executar ações na AWS é considerada uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS usa as permissões da entidade principal chamando um AWS service (Serviço da AWS), bem como o AWS service (Serviço da AWS) solicitante, para fazer solicitações para serviços subsequentes. As solicitações de FAS são feitas somente quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.
  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
  - Perfil vinculado a serviço: um perfil vinculado a serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode presumir o perfil para executar uma ação em seu nome. Perfis vinculadas ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados a serviço.
- Aplicações em execução no Amazon EC2: é possível usar um perfil do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer

solicitações da AWS CLI ou da API da AWS. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir um perfil da AWS a uma instância do EC2 e disponibilizá-la para todas as suas aplicações, crie um perfil de instância que esteja anexado a ela. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso na AWS criando políticas e anexando-as a identidades ou recursos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou recurso, define suas permissões. A AWS avalia essas políticas quando uma entidade principal (usuário, usuário-raiz ou sessão de perfil) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada na AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

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

Por padrão, usuários e perfis não têm permissões. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de perfis do AWS Management Console, da AWS CLI ou da API AWS.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas independentes que podem ser anexadas a vários usuários, grupos e perfis na Conta da AWS. As políticas gerenciadas incluem políticas gerenciadas pela AWS e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. As entidades principais podem incluir contas, usuários, funções, usuários federados ou Serviços da AWS.

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Não é possível usar as políticas gerenciadas pela AWS do IAM em uma política baseada em atributos.

Listas de controle de acesso (ACLs)

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

Amazon S3, AWS WAF e Amazon VPC são exemplos de serviços que oferecem compatibilidade com ACLs. Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

A AWS oferece compatibilidade com tipos de política menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade.

As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.

- Políticas de controle de serviço (SCPs): SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (UO) no AWS Organizations. O AWS Organizations é um serviço que agrupa e gerencia centralmente várias Contas da AWS pertencentes a sua empresa. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. A SCP limita as permissões para entidades em contas de membros, o que inclui cada Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizations e SCPs, consulte Service control policies no Guia do usuário do AWS Organizations.
- Políticas de controle de recursos (RCPs): RCPs são políticas JSON que podem ser usadas para definir o máximo de permissões disponíveis para recursos em suas contas sem atualizar as políticas do IAM anexadas a cada recurso que você possui. A RCP limita as permissões para recursos nas contas-membro e pode afetar as permissões efetivas para identidades, incluindo o Usuário raiz da conta da AWS, independentemente de pertencerem a sua organização. Consulte mais informações sobre o Organizations e as RCPs, incluindo uma lista de Serviços da AWS compatível com RCPs em Resource control policies (RCPs) no Guia do usuário do AWS Organizations.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recursos. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como a AWS determina se deve permitir uma solicitação quando há vários tipos de política envolvidos, consulte Lógica da avaliação de políticas no Manual do usuário do IAM.

Como a Amazon VPC funciona com o IAM

Antes de usar o IAM para gerenciar o acesso à Amazon VPC, você deve entender quais recursos do IAM estão disponíveis para uso com a Amazon VPC. Para obter uma visualização de alto nível de como a Amazon VPC e outros serviços da AWS funcionam com o IAM, consulte Serviços da AWS compatíveis com o IAM no Guia do usuário do IAM.

Tópicos

Com políticas do IAM baseadas em identidade, é possível especificar ações permitidas ou negadas. Para algumas ações, você pode especificar os recursos e condições sob os quais as ações são permitidas ou negadas. A Amazon VPC oferece suporte a ações, chaves de condição e recursos específicos. Para saber mais sobre todos os elementos usados em uma política JSON, consulte Referência de elementos de política JSON do IAM no Guia do usuário do IAM.

Ações

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

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. As ações de políticas geralmente têm o mesmo nome que a operação de API da AWS associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Inclua ações em uma política para conceder permissões para executar a operação associada.

A Amazon VPC compartilha o próprio namespace de API com o Amazon EC2. As ações de política na Amazon VPC usam o seguinte prefixo antes da ação: `ec2:`. Por exemplo, para conceder permissão a um usuário para criar uma VPC usando a operação de API `CreateVpc`, conceda

acesso à ação `ec2:CreateVpc`. As instruções de política devem incluir um elemento `Action` ou `NotAction`.

Para especificar várias ações em uma única declaração, separe-as com vírgulas, conforme exibido no exemplo a seguir.

```
"Action": [
      "ec2:action1",
      "ec2:action2"
]
```

Você também pode especificar várias ações usando caracteres curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `Describe`, inclua a ação a seguir:

```
"Action": "ec2:Describe*"
```

Para ver uma lista de ações de VPC da Amazon, consulte Ações definidas pelo Amazon EC2 na Referência de autorização do serviço.

Recursos

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

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

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

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

O recurso da VPC tem o ARN exibido no exemplo a seguir.

```
arn:${Partition}:ec2:${Region}:${Account}:vpc/${VpcId}
```

Por exemplo, para especificar a VPC `vpc-1234567890abcdef0` na instrução, use o ARN exibido no exemplo a seguir.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-1234567890abcdef0"
```

Para especificar todas as VPCs em uma Região específica que pertencem a uma conta específica, use o caractere curinga (*).

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/*"
```

Algumas ações da Amazon VPC, como as de criação de recursos, não podem ser executadas em um recurso específico. Nesses casos, você deve usar o caractere curinga (*).

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

Muitas ações da API do Amazon EC2 envolvem vários recursos. Para especificar vários recursos em uma única declaração, separe os ARNs com vírgulas.

```
"Resource": [
      "resource1",
      "resource2"
]
```

Para ver uma lista de tipos de recursos de VPC da Amazon e seus ARNs, consulte Recursos definidos pelo Amazon EC2 na Referência de autorização do serviço.

Chaves de condição

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

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

Se você especificar vários elementos de `Condition` em uma declaração ou várias chaves em um único elemento de `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você

especificar vários valores para uma única chave de condição, a AWS avaliará a condição usando uma operação lógica `OR`. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

A AWS oferece compatibilidade com chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição globais da AWS, consulte Chaves de contexto de condição globais da AWS no Guia do usuário do IAM.

Todas as ações do Amazon EC2 oferecem suporte às chaves de condição `aws:RequestedRegion` e `ec2:Region`. Para obter mais informações, consulte Exemplo: restringir acesso a uma região específica.

A Amazon VPC define seu próprio conjunto de chaves de condição e também oferece suporte ao uso de algumas chaves de condição globais. Para ver uma lista de chaves de condição de VPC da Amazon, consulte Chaves de condição do Amazon EC2 na Referência de autorização do serviço. Para saber com quais ações e recursos é possível usar a chave de condição, consulte Ações definidas pelo Amazon EC2.

Políticas baseadas em recursos da Amazon VPC

As políticas baseadas em recursos são documentos de políticas JSON que especificam quais ações uma entidade principal pode executar no recurso da Amazon VPC e sob quais condições.

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recurso. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso estão em diferentes contas da AWS, você também deve conceder à entidade principal permissão para acessar o recurso. Conceda permissão anexando uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Autorização baseada em tags

É possível anexar tags a recursos da Amazon VPC ou passar tags em uma solicitação. Para controlar o acesso com base em tags, forneça informações sobre as tags no elemento de condição de uma política usando chaves de condição. Para obter mais informações, consulte Conceder permissão para marcar recursos durante a criação no Manual do usuário do Amazon EC2 para instâncias do Linux.

Para visualizar um exemplo de política baseada em identidade que visa limitar o acesso a um recurso baseado nas tags desse recurso, consulte Executar instâncias em uma VPC específica.

Perfis do IAM

Um perfil do IAM é uma entidade dentro da sua Conta da AWS que tem permissões específicas.

Usar credenciais temporárias

É possível usar credenciais temporárias para fazer login com federação, assumir uma função do IAM ou assumir uma função entre contas. As credenciais de segurança temporárias são obtidas chamando operações da API do AWS STS, como AssumeRole ou GetFederationToken.

A Amazon VPC oferece suporte ao uso de credenciais temporárias.

Funções vinculadas ao serviço

Perfis vinculados ao serviço permitem que os serviços da AWS acessem recursos em outros serviços para concluir uma ação em seu nome. Os perfis vinculados a serviço aparecem em sua conta do IAM e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para funções vinculadas ao serviço.

Os Gateways de trânsito oferecem suporte às funções vinculadas ao serviço.

Funções de serviço

Esse atributo permite que um serviço assuma um perfil de serviço em seu nome. O perfil permite que o serviço acesse recursos em outros serviços para concluir uma ação em seu nome. Os perfis de serviço aparecem em sua conta do IAM e são de propriedade da conta. Isso significa que um administrador do IAM pode alterar as permissões para esse perfil. Porém, fazer isso pode alterar a funcionalidade do serviço.

A Amazon VPC oferece suporte a funções de serviço para logs de fluxo. Ao criar um log de fluxo, você deve selecionar uma função que permita que o serviço de log de fluxo acesse o CloudWatch

Logs. Para ter mais informações, consulte the section called “Perfil do IAM para publicar logs de fluxo no CloudWatch Logs”.

Exemplos de políticas da Amazon VPC

Por padrão, os perfis do IAM não têm permissão para criar ou modificar recursos da VPC. Eles também não podem executar tarefas usando o AWS Management Console, a AWS CLI ou uma API da AWS. Um administrador do IAM deve criar políticas do IAM que concedam aos perfis permissão para executarem operações de API específicas nos recursos especificados de que precisam. O administrador deve anexar as políticas aos perfis do IAM que exijam essas permissões.

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

Conteúdo

Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos da Amazon VPC em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo: para começar a conceder permissões a seus usuários e workloads, use as políticas gerenciadas pela AWS, que concedem permissões para muitos casos de uso comuns. Elas estão

disponíveis em seus Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da AWS que são específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.

- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Também pode usar condições para conceder acesso a ações de serviço, se elas forem usadas por meio de um AWS service (Serviço da AWS) específico, como o AWS CloudFormation. Para obter mais informações, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA): se houver um cenário que exija usuários do IAM ou um usuário raiz em sua Conta da AWS, ative a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

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

Use o console da Amazon VPC.

Para acessar o console da Amazon VPC, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir listar e visualizar detalhes sobre os recursos da Amazon VPC em sua conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva que as

permissões mínimas necessárias, o console não funcionará como pretendido para entidades (perfis do IAM) com essa política.

A política a seguir concede permissão a um perfil para listar recursos no console da VPC, mas não para criá-los, atualizá-los ou excluí-los.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeClassicLinkInstances",
                "ec2:DescribeClientVpnEndpoints",
                "ec2:DescribeCustomerGateways",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeEgressOnlyInternetGateways",
                "ec2:DescribeFlowLogs",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeManagedPrefixLists",
                "ec2:DescribeMovingAddresses",
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePrefixLists",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroupReferences",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeStaleSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeTrafficMirrorFilters",
                "ec2:DescribeTrafficMirrorSessions",
                "ec2:DescribeTrafficMirrorTargets",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeTransitGatewayVpcAttachments",
                "ec2:DescribeTransitGatewayRouteTables",
```

```
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcEndpointConnectionNotifications",
                "ec2:DescribeVpcEndpointConnections",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:GetManagedPrefixListAssociations",
                "ec2:GetManagedPrefixListEntries"
            ],
            "Resource": "*"
        }
    ]
}
```

Não é necessário conceder permissões mínimas do console para perfis que fazem chamadas somente à AWS CLI ou à API da AWS. Em vez disso, permita o acesso somente às ações que correspondem à operação da API que o perfil precisa executar.

Criar uma VPC com uma sub-rede pública

O exemplo a seguir permite que os perfis criem VPCs, sub-redes, tabelas de rota e gateways da Internet. Os perfis também podem anexar um gateway da Internet a uma VPC e criar rotas em tabelas de rotas. A ação `ec2:ModifyVpcAttribute` permite que os perfis habilitem nomes de host DNS para a VPC, para que cada instância executada nessa VPC receba um nome de host DNS.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
```

```
        "ec2:CreateInternetGateway",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:ModifyVpcAttribute"
      ],
      "Resource": "*"
    }
   ]
}
```

A política anterior também permite que os perfis criem uma VPC no console da Amazon VPC.

Modificar e excluir recursos da VPC

É possível controlar os recursos da VPC que os perfis podem modificar ou excluir. Por exemplo, a política a seguir permite que os perfis trabalhem com e excluam tabelas de rotas com a etiqueta `Purpose=Test`. A política também especifica que os perfis podem excluir somente os gateways da Internet que tenham a etiqueta `Purpose=Test`. Os perfis não podem trabalhar com tabelas de rota ou gateways da Internet que não tenham essa etiqueta.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteInternetGateway",
            "Resource": "arn:aws:ec2:*:*:internet-gateway/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Purpose": "Test"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteRouteTable",
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:route-table/*",
            "Condition": {
```

```
                "StringEquals": {
                    "ec2:ResourceTag/Purpose": "Test"
                }
            }
        }
    ]
}
```

Gerenciar grupos de segurança

A política a seguir permite que os perfis gerenciem grupos de segurança. A primeira instrução permite que os perfis excluam qualquer grupo de segurança com a etiqueta `Stack=test` e gerenciem as regras de entrada e saída para qualquer grupo de segurança com a etiqueta `Stack=test`. A segunda instrução requer que os perfis marquem qualquer grupo de segurança criado com a etiqueta `Stack=Test`. A terceira instrução permite que os perfis criem etiquetas ao criar um grupo de segurança. A quarta instrução permite que os perfis visualizem qualquer grupo de segurança e regra de grupo de segurança. A quinta instrução permite aos perfis criar um grupo de segurança em uma VPC.

> **Note**
>
> Essa política não pode ser usada pelo serviço do AWS CloudFormation para criar um grupo de segurança com as tags necessárias. Se você remover a condição da ação `ec2:CreateSecurityGroup` que exige a tag, a política funcionará.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup",
                "ec2:ModifySecurityGroupRules",
                "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
            ],
```

```
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Stack": "test"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Stack": "test"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "Stack"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSecurityGroup"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeVpcs",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:vpc/*"
        }
```

```
    ]
}
```

Para permitir que os perfis alterem o grupo de segurança associado a uma instância, adicione a ação `ec2:ModifyInstanceAttribute` à sua política.

Para permitir que os perfis alterem grupos de segurança de uma interface de rede, adicione a ação `ec2:ModifyNetworkInterfaceAttribute` à sua política.

Gerenciar regras de grupos de segurança

A política a seguir concede aos perfis permissão para visualizar todos os grupos de segurança e regras de grupo de segurança, adicionar e remover regras de entrada e de saída para os grupos de segurança de uma VPC específica e modificar descrições de regras para a VPC especificada. A primeira declaração usa a chave de condição `ec2:Vpc` para permissões de escopo para uma VPC específica.

A segunda instrução concede permissão aos perfis para descrever todos os grupos de segurança, regras do grupo de segurança e etiquetas. Isso permite que os perfis visualizem as regras de grupo de segurança a fim de modificá-las.

```
{
  "Version": "2012-10-17",
  "Statement":[{
    "Effect":"Allow",
    "Action": [
       "ec2:AuthorizeSecurityGroupIngress",
       "ec2:RevokeSecurityGroupIngress",
       "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
       "ec2:AuthorizeSecurityGroupEgress",
       "ec2:RevokeSecurityGroupEgress",
       "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
       "ec2:ModifySecurityGroupRules"
    ],
     "Resource": "arn:aws:ec2:region:account-id:security-group/*",
      "Condition": {
        "ArnEquals": {
          "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-id"
        }
      }
    },
    {
```

```
      "Effect": "Allow",
      "Action": [
          "ec2:DescribeSecurityGroups",
          "ec2:DescribeSecurityGroupRules",
          "ec2:DescribeTags"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
          "ec2:ModifySecurityGroupRules"
      ],
      "Resource": "arn:aws:ec2:region:account-id:security-group-rule/*"
    }
  ]
}
```

Executar instâncias em uma sub-rede específica

A política a seguir concede permissões aos perfis para executar instâncias em uma sub-rede específica e usar um grupo de segurança específico na solicitação. A política faz isso especificando o ARN para a sub-rede e o ARN para o grupo de segurança. Se perfis tentarem executar uma instância em uma sub-rede diferente ou usar um grupo de segurança diferente, haverá falha na solicitação (a menos que outra política ou instrução conceda aos perfis permissão para fazer isso).

A política também concede permissão para usar o recurso de interface de rede. Quando executada em uma sub-rede, a solicitação `RunInstances` cria uma interface de rede primária por padrão, para que o perfil precise de permissão para criar esse recurso ao executar a instância.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region::image/ami-*",
        "arn:aws:ec2:region:account:instance/*",
        "arn:aws:ec2:region:account:subnet/subnet-id",
        "arn:aws:ec2:region:account:network-interface/*",
        "arn:aws:ec2:region:account:volume/*",
        "arn:aws:ec2:region:account:key-pair/*",
```

```
        "arn:aws:ec2:region:account:security-group/sg-id"
      ]
    }
  ]
}
```

Executar instâncias em uma VPC específica

A política a seguir concede permissões aos perfis para executar instâncias em qualquer sub-rede de uma VPC específica. A política faz isso, aplicando uma chave de condição (`ec2:Vpc`) ao recurso de sub-rede.

A política também concede permissão aos perfis para executar instâncias usando somente AMIs que possuam a etiqueta "`department=dev`".

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:region:account-id:subnet/*",
        "Condition": {
         "ArnEquals": {
            "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-id"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:region::image/ami-*",
      "Condition": {
         "StringEquals": {
            "ec2:ResourceTag/department": "dev"
            }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account:instance/*",
         "arn:aws:ec2:region:account:volume/*",
```

```
            "arn:aws:ec2:region:account:network-interface/*",
            "arn:aws:ec2:region:account:key-pair/*",
            "arn:aws:ec2:region:account:security-group/*"
            ]
        }
    ]
}
```

Bloquear o acesso público a VPCs e sub-redes

Os exemplos de política a seguir concedem aos perfis permissão para trabalhar com o atributo Bloquear o Acesso Público (BPA) da VPC para bloquear o acesso público a recursos em VPCs e sub-redes.

Exemplo 1: permitir o acesso somente para leitura às configurações do BPA da VPC e exclusões do BPA da VPC no âmbito total da conta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VPCBPAReadOnlyAccess",
      "Action": [
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeVpcBlockPublicAccessExclusions"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Exemplo 2: permitir total acesso para leitura e gravação às configurações do BPA da VPC e exclusões do BPA da VPC no âmbito total da conta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VPCBPAFullAccess",
      "Action": [
        "ec2:DescribeVpcBlockPublicAccessOptions",
```

```
        "ec2:DescribeVpcBlockPublicAccessExclusions",
        "ec2:ModifyVpcBlockPublicAccessOptions",
        "ec2:CreateVpcBlockPublicAccessExclusion",
        "ec2:ModifyVpcBlockPublicAccessExclusion",
        "ec2:DeleteVpcBlockPublicAccessExclusion"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Exemplo 3: permitir acesso a todas as APIs do EC2, exceto para modificar as configurações do BPA da VPC e criar exclusões.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EC2FullAccess"
      "Action": [
        "ec2:*",
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Sid": "VPCBPAPartialAccess",
      "Action": [
        "ec2:ModifyVpcBlockPublicAccessOptions",
        "ec2:CreateVpcBlockPublicAccessExclusion"
      ],
      "Effect": "Deny",
      "Resource": "*"
    }
  ]
}
```

Exemplos adicionais de políticas da Amazon VPC

É possível encontrar políticas do IAM de exemplo adicionais relacionadas à Amazon VPC na documentação a seguir:

- Listas de prefixos gerenciados
- Espelhamento de tráfego
- Gateways de trânsito
- Endpoints da VPC e serviços de endpoint da VPC (AWS PrivateLink)
- Emparelhamento de VPC

Solução de problemas de identidade e acesso da Amazon VPC

Use as informações a seguir para ajudar a diagnosticar e corrigir problemas comuns que você possa encontrar ao trabalhar com a Amazon VPC e o IAM.

Problemas

- Não tenho autorização para executar uma ação na Amazon VPC
- Não estou autorizado a executar iam:PassRole
- Quero permitir que pessoas fora da minha conta da AWS acessem meus recursos da Amazon VPC

Não tenho autorização para executar uma ação na Amazon VPC

Se o AWS Management Console informar que você não está autorizado a executar uma ação, você deverá entrar em contato com o administrador para obter assistência. Seu administrador é a pessoa que forneceu a você suas credenciais de início de sessão.

O exemplo de erro a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre uma sub-rede, mas pertence a um perfil do IAM que não tem as permissões `ec2:DescribeSubnets`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:DescribeSubnets on resource: subnet-id
```

Nesse caso, Mateo pede ao administrador para atualizar a política para permitir que ele acesse a sub-rede.

Não estou autorizado a executar iam:PassRole

Caso receba uma mensagem de erro informando que você não tem autorização para executar a ação `iam:PassRole`, suas políticas deverão ser atualizadas para permitir a transmissão de uma função à Amazon VPC.

Alguns Serviços da AWS permitem que você passe um perfil existente para o serviço, em vez de criar um perfil de serviço ou perfil vinculado ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O erro exemplificado a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta usar o console para executar uma ação na Amazon VPC. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se você precisar de ajuda, entre em contato com seu administrador AWS. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha conta da AWS acessem meus recursos da Amazon VPC

Você pode criar uma função que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem compatibilidade com políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte o seguinte:

- Para saber se a Amazon VPC oferece suporte a esses recursos, consulte Como a Amazon VPC funciona com o IAM.
- Para saber como conceder acesso a seus recursos em todas as Contas da AWS pertencentes a você, consulte Fornecimento de acesso a um usuário do IAM em outra Conta da AWS pertencente a você no Guia de usuário do IAM.

- Para saber como conceder acesso a seus recursos para Contas da AWS de terceiros, consulte Fornecimento de acesso a Contas da AWS pertencentes a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Políticas gerenciadas da AWS para Amazon Virtual Private Cloud

Uma política gerenciada pela AWS é uma política independente criada e administrada pela AWS. As políticas gerenciadas pela AWS são criadas para fornecer permissões a vários casos de uso comuns e permitir a atribuição de permissões a usuários, grupos e perfis.

Lembre-se de que as políticas gerenciadas pela AWS podem não conceder permissões de privilégio mínimo para casos de uso específicos, por estarem disponíveis para uso por todos os clientes da AWS. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas em políticas gerenciadas pela AWS. Se a AWS atualiza as permissões definidas em um política gerenciada por AWS, a atualização afeta todas as identidades de entidades principais (usuários, grupos e perfis) às quais a política estiver vinculada. É provável que a AWS atualize uma política gerenciada por AWS quando um novo AWS service (Serviço da AWS) for lançado, ou novas operações de API forem disponibilizadas para os serviços existentes.

Para obter mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

Política gerenciada pela AWS: AmazonVPCFullAccess

Você pode anexar a política `AmazonVPCFullAccess` a suas identidades do IAM. Essa política concede permissões que possibilitam acesso total à Amazon VPC.

Para visualizar as permissões para esta política, consulte AmazonVPCFullAccess na Referência de políticas gerenciadas da AWS.

Política gerenciada pela AWS: AmazonVPCReadOnlyAccess

Você pode anexar a política `AmazonVPCReadOnlyAccess` a suas identidades do IAM. Esta política concede permissões que oferecem acesso somente leitura à Amazon VPC.

Para visualizar as permissões para esta política, consulte AmazonVPCReadOnlyAccess na Referência de políticas gerenciadas da AWS.

Política gerenciada pela AWS: AmazonVPCCrossAccountNetworkInterfaceOperations

É possível anexar a política `AmazonVPCCrossAccountNetworkInterfaceOperations` às identidades do IAM. Essa política concede permissões com as quais a identidade pode criar interfaces de rede e as anexar a recursos entre contas.

Para visualizar as permissões para esta política, consulte AmazonVPCCrossAccountNetworkInterfaceOperations na Referência de políticas gerenciadas da AWS.

Atualizações da Amazon VPC para políticas gerenciadas pela AWS

Visualize detalhes sobre atualizações em políticas gerenciadas pela AWS para a Amazon VPC desde que este serviço começou a rastrear essas alterações em março de 2021.

Alteração	Descrição	Data
the section called “AmazonVPCFullAccess”: atualizar para uma política existente	As ações AssociateSecurityGroupVpc, DescribeSecurityGroupVpcAssociations e DisassociateSecurityGroupVpc foram adicionadas, permitindo associar, desassociar e visualizar associações de grupos de segurança com VPCs.	9 de dezembro de 2024
the section called “AmazonVPCReadOnlyAccess”: atualizar para uma política existente	A ação DescribeSecurityGroupVpcAssociations foi adicionada, permitindo visualizar as associações de	9 de dezembro de 2024

Alteração	Descrição	Data
	grupos de segurança com VPCs.	
the section called “AmazonVPCFullAccess”: atualizar para uma política existente	Foi adicionada a ação GetSecurityGroupsForVpc, que permite obter grupos de segurança que podem ser usados em sua VPC.	8 de fevereiro de 2024
the section called “AmazonVPCReadOnlyAccess”: atualizar para uma política existente	Foi adicionada a ação GetSecurityGroupsForVpc, que permite obter grupos de segurança que podem ser usados em sua VPC.	8 de fevereiro de 2024
the section called “AmazonVPCCrossAccountNetworkInterfaceOperations”: atualizar para uma política existente	Foram adicionadas as ações AssignIpv6Addresses e UnassignIpv6Addresses, que permitem gerenciar os endereços IPv6 associados às interfaces de rede.	25 de setembro de 2023
the section called “AmazonVPCReadOnlyAccess”: atualizar para uma política existente	Adicionada a ação DescribeSecurityGroupRules, que permite a visualização das regras do grupo de segurança.	2 de agosto de 2021
the section called “AmazonVPCFullAccess”: atualizar para uma política existente	Adicionadas as ações DescribeSecurityGroupRules e ModifySecurityGroupRules, que permitem a visualização e a modificação das regras do grupo de segurança.	2 de agosto de 2021

Alteração	Descrição	Data
the section called “AmazonVPCFullAccess”: atualizar para uma política existente	Ações adicionadas para gateways de operadoras, grupos de IPv6, gateways locais e tabelas de rota de gateways locais.	23 de junho de 2021
the section called “AmazonVPCReadOnlyAccess”: atualizar para uma política existente	Ações adicionadas para gateways de operadoras, grupos de IPv6, gateways locais e tabelas de rota de gateways locais.	23 de junho de 2021

Segurança da infraestrutura no Amazon S3

Como um serviço gerenciado, o Amazon Private Virtual Cloud é protegido pela segurança da rede global da AWS. Para obter informações sobre serviços de segurança da AWS e como a AWS protege a infraestrutura, consulte Segurança na Nuvem AWS. Para projetar seu ambiente da AWS usando as práticas recomendadas de segurança da infraestrutura, consulte Proteção de Infraestrutura em Pilar de Segurança: AWS Estrutura bem arquitetada.

Você usa as chamadas de API publicadas da AWS para acessar a Amazon VPC por meio da rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou é possível usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Isolamento de rede

Uma nuvem virtual privada (VPC) é uma rede virtual na área isolada logicamente na Nuvem AWS. Use VPCs separadas para isolar a infraestrutura por workload ou entidade organizacional.

Uma sub-rede é um intervalo de endereços IP em uma VPC. Quando executa uma instância, você a executa em uma sub-rede em sua VPC. Use sub-redes para isolar as camadas de sua aplicação (por exemplo, Web, aplicação e banco de dados) em uma única VPC. Use sub-redes privadas para as instâncias que não devem ser acessadas diretamente pela Internet.

É possível usar AWS PrivateLink para habilitar recursos em sua VPC para se conectar aos Serviços da AWS usando endereços IP privados, como se esses serviços estivessem hospedados diretamente em sua VPC. Portanto, você não precisa usar um gateway da Internet ou um dispositivo NAT para acessar os Serviços da AWS.

Controlar o tráfego de rede

Considere as seguintes opções para controlar o tráfego de rede para os recursos em sua VPC, por exemplo, instâncias do EC2:

- Use grupos de segurança como mecanismo primário para controlar o acesso à rede a suas VPCs. Quando necessário, use ACLs de rede para fornecer controle de rede sem estado e de alta granularidade. Os grupos de segurança são mais versáteis que as ACLs de rede devido à capacidade de realizar a filtragem de pacotes com estado e criar regras que fazem referência a outros grupos de segurança. As ACLs de rede podem ser eficientes como controle secundário (por exemplo, para negar um subconjunto de tráfego específico) ou como grades de proteção de sub-rede de alto nível. Além disso, como as ACLs de rede se aplicam a toda uma sub-rede, elas poderão ser usadas como defesa mais profunda caso uma instância seja iniciada sem um grupo de segurança correto.
- Use sub-redes privadas para as instâncias que não devem ser acessadas diretamente pela Internet. Use um bastion host ou gateway NAT para acessar a Internet em uma instância em sub-redes privadas.
- Configure tabelas de rotas de sub-rede com as rotas de rede mínimas para suportar seus requisitos de conectividade.
- Considere usar grupos de segurança adicionais ou interfaces de rede para controlar e auditar o tráfego de gerenciamento de instâncias do Amazon EC2 separadamente do tráfego de aplicação regular. Assim, é possível implementar políticas do IAM especiais para controle de alterações, facilitando a auditoria de alterações às regras de grupo de segurança ou scripts automáticos de

verificação de regras. Várias interfaces de rede também fornecem opções adicionais para controlar o tráfego de rede, incluindo a capacidade de criar políticas de roteamento baseado em host ou usar diferentes regras de roteamento de sub-rede da VPC com base na interface de rede atribuída a uma sub-rede.

- Use o AWS Virtual Private Network ou o AWS Direct Connect para estabelecer conexões privadas de suas redes remotas com suas VPCs. Para obter mais informações, consulte Network-to-Amazon VPC connectivity options (Opções de conectividade entre a rede e a Amazon VPC).
- Use Logs de fluxo da VPC para monitorar o tráfego recebido nas instâncias.
- Use o AWS Security Hub para verificar acessibilidade de rede acidental nas instâncias.
- Use AWS Network Firewall para proteger as sub-redes na sua VPC contra ameaças comuns de rede.

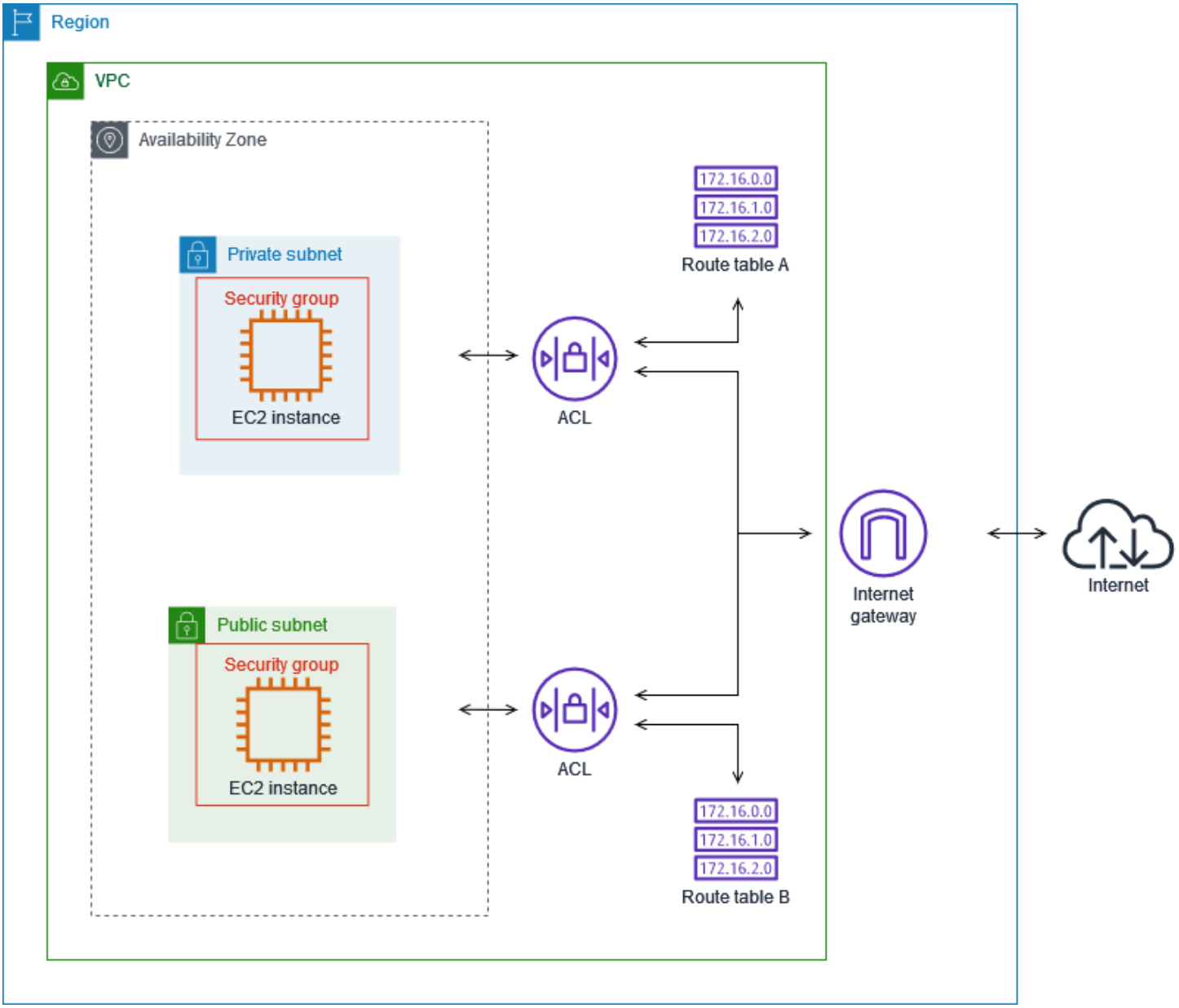
Comparar grupos de segurança e ACLs de rede

A tabela a seguir resume as diferenças básicas entre grupos de segurança e ACLs de rede.

Grupo de segurança	Conexão ACL
Opera em nível de instância	Opera em nível de sub-rede
Aplica-se a uma instância somente se ela estiver associada à instância	Aplica-se a todas as instâncias implantadas na sub-rede associada (fornecendo uma camada adicional de defesa, caso as regras do grupo de segurança sejam permissivas demais)
Comporta apenas regras de permissão	Comporta regras de permissão e negação
Avalia todas as regras antes de decidir se deve permitir o tráfego	Avalia as regras na ordem, a partir da regra de número mais baixo, ao decidir se o tráfego será permitido ou não
Com estado: o tráfego de retorno é permitido, seja qual for a regra	Sem estado: o tráfego de deve ser permitido explicitamente pelas regras

O diagrama a seguir mostra as camadas de segurança fornecidas por grupos de segurança e ACLs de rede. Por exemplo, o tráfego para e proveniente de um gateway da Internet é roteado

para a sub-rede apropriada usando as rotas apresentadas na tabela de rotas. As regras da ACL de rede associadas à sub-rede controlam qual tráfego é permitido à sub-rede. As regras do grupo de segurança associadas à instância controlam qual tráfego é permitido à instância.



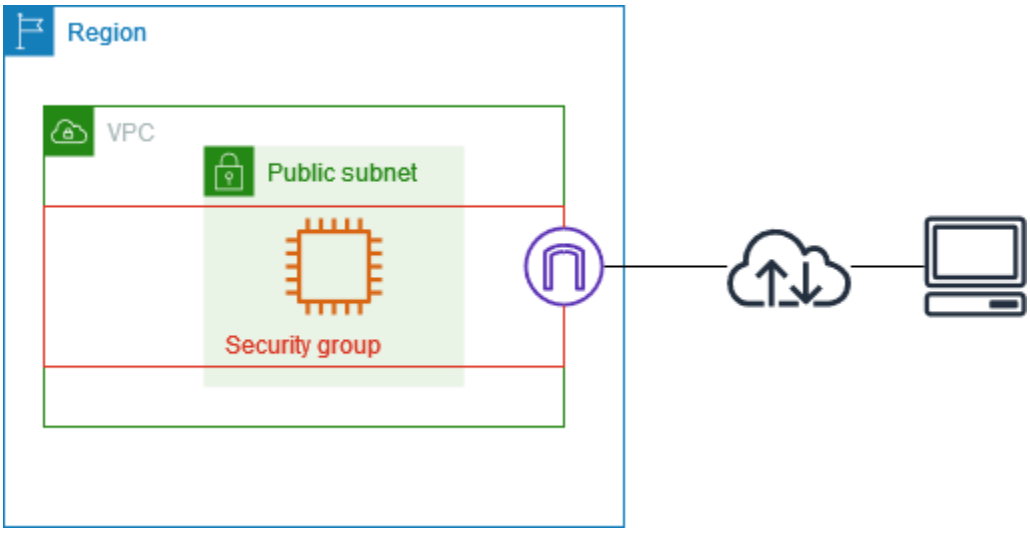
É possível proteger as instâncias usando somente grupos de segurança. No entanto, é possível adicionar ACLs de rede como uma camada adicional de defesa. Para ter mais informações, consulte Exemplo: controlar o acesso a instâncias em uma sub-rede.

Controle o tráfego para seus recursos da AWS usando grupos de segurança

Um grupo de segurança controla o tráfego que tem permissão para acessar e sair dos recursos aos quais está associado. Por exemplo, depois de associar um grupo de segurança a uma instância do EC2, ele controla o tráfego de entrada e saída da instância.

Quando você cria uma VPC, ela vem com um grupo de segurança padrão. É possível criar grupos de segurança adicionais para uma VPC, cada um com suas próprias regras de entrada e saída. Você pode especificar a origem, o intervalo de portas e o protocolo de cada regra de entrada. Você pode especificar o destino, o intervalo de portas e o protocolo de cada regra de saída.

O diagrama a seguir mostra uma VPC com uma sub-rede, um gateway da Internet e um grupo de segurança. A sub-rede contém uma instância do EC2. O grupo de segurança é atribuído à instância. O grupo de segurança atua como um firewall virtual. O único tráfego que chega à instância é aquele permitido pelas regras do grupo de segurança. Por exemplo, se o grupo de segurança contiver uma regra que permita o tráfego ICMP proveniente da sua rede para a instância, você poderá efetuar ping na instância a partir do computador. Se o grupo de segurança não contiver uma regra que permita tráfego SSH, não será possível conectar-se à instância via SSH.



Conteúdo

- Crie um grupo de segurança para a VPC
- Configurar regras de grupo de segurança
- Exclua um grupo de segurança
- Associar grupos de segurança a várias VPCs
- Compartilhar grupos de segurança com o AWS Organizations

Preços

Não há cobrança adicional pelo uso de grupos de segurança.

Noções básicas do grupo de segurança

- Você poderá atribuir um grupo de segurança a recursos criados na mesma VPC do grupo de segurança ou a recursos em outras VPCs se utilizar o recurso Associação de VPC do grupo de segurança para associar o grupo de segurança a outras VPCs na mesma região. Você também pode atribuir vários grupos de segurança a um único recurso.
- Ao criar um grupo de segurança, você deve fornecer um nome e uma descrição. As seguintes regras se aplicam:
  - O nome do grupo de segurança deve ser exclusivo dentro da VPC.
  - Os nomes e as descrições podem ter até 255 caracteres de comprimento.
  - Os nomes e as descrições são limitados aos seguintes caracteres: a-z, A-Z, 0-9, espaços e ._-:/()#,@[]+=&;{}!$*.
  - Quando o nome termina com espaços, cortamos os espaços existentes no final do nome. Por exemplo, se você inserir “Testar grupo de segurança " para o nome, nós o armazenaremos como “Testar grupo de segurança”.
  - Um nome de grupo de segurança não pode começar com `sg-`.
- Os grupos de segurança são com estado. Por exemplo, se você enviar uma solicitação de uma instância, o tráfego de resposta dessa solicitação terá permissão para alcançar a instância, independentemente das regras do grupo de segurança de entrada. As respostas ao tráfego de entrada permitido têm permissão para deixar a instância, independentemente das regras de saída.
- Os grupos de segurança não filtram tráfego de entrada ou de saída de:
  - Serviços de nomes de domínio (DNS) da Amazon
  - Dynamic Host Configuration Protocol (DHCP – Protocolo de configuração de host dinâmico) da Amazon

  - Metadados da instância do Amazon EC2
  - Endpoints de metadados de tarefas do Amazon ECS
  - Ativação de licença para instâncias do Windows
  - Serviço de Sincronização Temporal da Amazon
  - Endereços IP reservados usados pelo roteador padrão da VPC
- Existem cotas no número de grupos de segurança que podem ser criados por VPC, o número de regras que podem ser adicionadas a cada grupo de segurança e o número de grupos de segurança que podem ser associadas a uma interface de rede. Para ter mais informações, consulte Cotas da Amazon VPC.

Práticas recomendadas

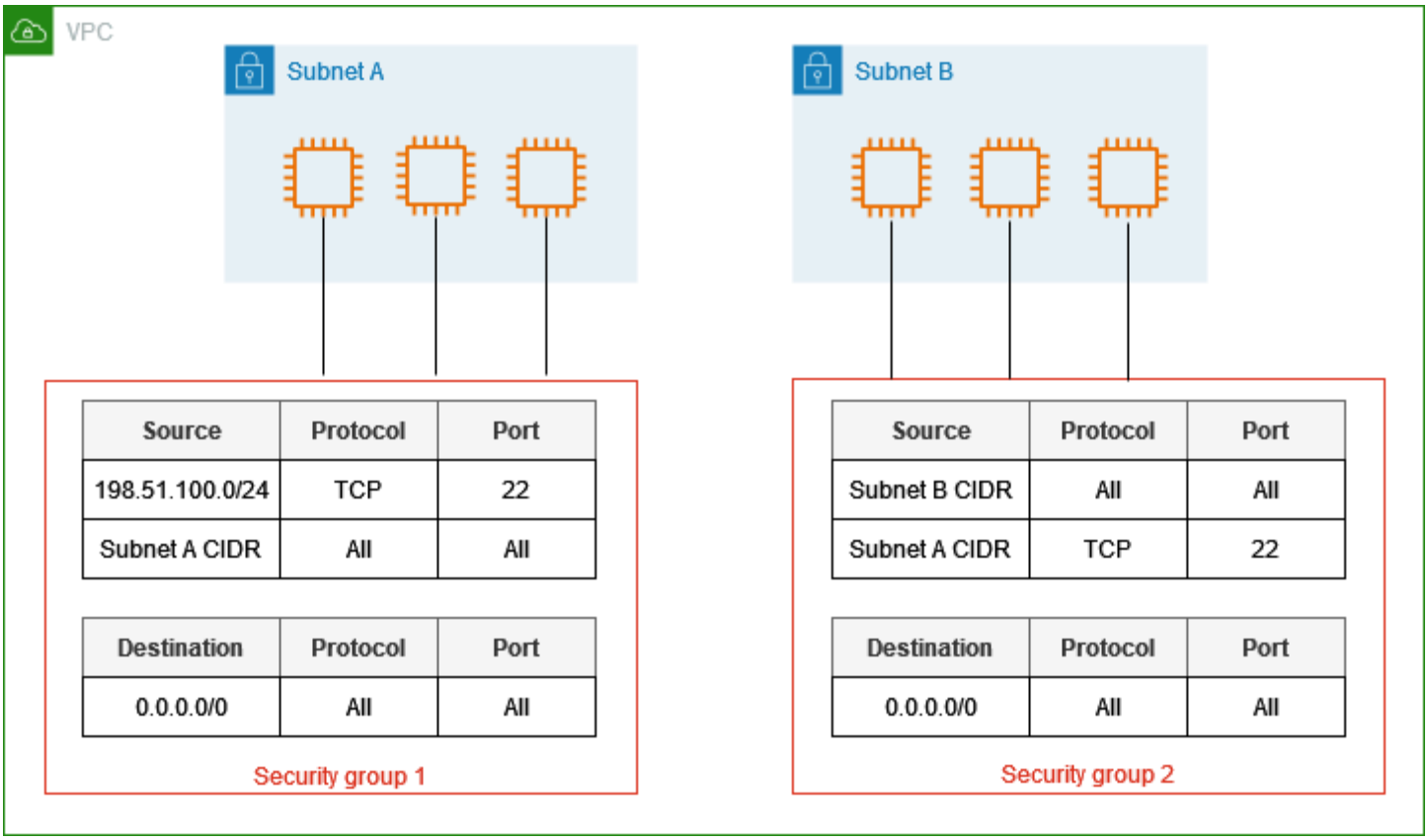
- Autorize somente entidades principais específicas do IAM para criar e modificar grupos de segurança.
- Crie o número mínimo de grupos de segurança necessários para diminuir o risco de erro. Use cada grupo de segurança para gerenciar o acesso a recursos que tenham funções e requisitos de segurança semelhantes.
- Quando você adicionar regras de entrada para as portas 22 (SSH) ou 3389 (RDP) para poder acessar as instâncias do EC2, autorize somente intervalos específicos de endereços IP. Se você especificar 0.0.0.0/0 (IPv4) e ::/ (IPv6), qualquer pessoa poderá acessar suas instâncias de qualquer endereço IP usando o protocolo especificado.
- Não abra grandes intervalos de portas. Certifique-se de que o acesso por meio de cada porta seja restrito às fontes ou destinos que o exigem.
- Você pode configurar ACLs da rede com regras semelhantes às dos grupos de segurança para adicionar uma camada de segurança à sua VPC. Para obter mais informações sobre as diferenças entre grupos de segurança e ACLs de rede, consulte Comparar grupos de segurança e ACLs de rede.

Exemplo de grupo de segurança

O diagrama a seguir mostra uma VPC com dois grupos de segurança e duas sub-redes. As instâncias na sub-rede A têm os mesmos requisitos de conectividade e, portanto, estão associadas ao grupo de segurança 1. As instâncias na sub-rede B têm os mesmos requisitos de conectividade

e, portanto, estão associadas ao grupo de segurança 2. As regras do grupo de segurança permitem tráfego da seguinte maneira:

- A primeira regra de entrada no grupo de segurança 1 permite tráfego SSH para as instâncias na sub-rede A a partir do intervalo de endereços especificado (por exemplo, um intervalo na sua própria rede).
- A segunda regra de entrada no grupo de segurança 1 permite que as instâncias na sub-rede A se comuniquem entre si usando qualquer protocolo e porta.
- A primeira regra de entrada no grupo de segurança 2 permite que as instâncias na sub-rede B se comuniquem entre si usando qualquer protocolo e porta.
- A segunda regra de entrada no grupo de segurança 2 permite que as instâncias na sub-rede A se comuniquem com as instâncias na sub-rede B via SSH.
- Ambos os grupos de segurança usam a regra de saída padrão, que permite todo o tráfego.



Regras de grupos de segurança

As regras de um grupo de segurança controlam o tráfego de entrada que tem permissão para alcançar as instâncias associadas ao grupo de segurança. As regras também controlam o tráfego de saída que pode deixá-los.

Você pode adicionar ou remover regras de um grupo de segurança (também conhecido como autorização ou revogação do acesso de entrada ou de saída). Uma regra aplica-se ao tráfego de entrada (ingresso) ou ao tráfego de saída (egresso). Você pode conceder acesso a uma origem ou destino específico.

Conteúdo

Noções básicas sobre grupos de segurança

As seguintes são as características das regras de grupos de segurança:

- Você pode especificar regras de permissão, mas não regras de negação.
- Quando você cria um grupo de segurança, ele não possui regras de entrada. Portanto, nenhum tráfego de entrada tem permissão até que você adicione regras de entrada ao grupo de segurança.
- Quando você cria um grupo de segurança pela primeira vez, ele possui uma regra de saída que permite todo o tráfego de saída do recurso. Você pode remover a regra e adicionar regras de saída que permitem somente tráfego de saída específico. Se o grupo de segurança não tiver nenhuma regra de saída, nenhum tráfego de saída será permitido.
- Quando você associa vários grupos de segurança a um recurso, as regras de cada grupo de segurança são agregadas para formar um único conjunto de regras, que é utilizado para determinar se o acesso deve ser permitido.
- Quando você adiciona, atualiza ou remove regras, elas são aplicadas automaticamente a todos os recursos associados ao grupo de segurança. Para obter instruções, consulte Configurar regras de grupo de segurança.

- O efeito de algumas alterações nas regras pode depender de como o tráfego é acompanhado. Para obter mais informações, consulte Rastreamento de conexão no Guia do usuário do Amazon EC2.
- Quando você cria uma regra para o grupo de segurança, a AWS atribui um ID exclusivo à regra. É possível usar o ID de uma regra ao usar a API ou a CLI para modificar ou excluir a regra.

Limitação

Os grupos de segurança não podem bloquear solicitações entre o DNS e o Route 53 Resolver, às vezes, chamado de "endereço IP VPC+2" (consulte Amazon Route 53 Resolver no Guia do desenvolvedor do Amazon Route 53) ou como AmazonProvidedDNS. Para filtrar solicitações de DNS usando o Route 53 Resolver, use o Route 53 Resolver DNS Firewall.

Componentes de uma regra de grupo de segurança

Estes são os componentes das regras de grupo de segurança de entrada e saída:

- Protocolo: o protocolo a permitir. Os protocolos mais comuns são 6 (TCP), 17 (UDP) e 1 (ICMP).
- Intervalo de portas: para TCP, UDP ou um protocolo personalizado, o intervalo de portas a ser permitido. É possível especificar um único número de porta (por exemplo, 22) ou um intervalo de números de portas (por exemplo, `7000-8000`).
- Tipo e código do ICMP: para o ICMP, o tipo e o código do ICMP. Por exemplo, use o tipo 8 para solicitação de eco ICMP ou digite 128 para solicitação de eco ICMPv6.
- Origem ou destino: a origem (regras de entrada) ou o destino (regras de saída) para permitir o tráfego. Especifique um dos seguintes:
  - Um endereço IPv4 único. Use o comprimento de prefixo `/32`. Por exemplo, `203.0.113.1/32`.
  - Um endereço IPv6 único. Use o comprimento de prefixo `/128`. Por exemplo, `2001:db8:1234:1a00::123/128`.
  - Um intervalo de endereços IPv4, em notação de bloco CIDR. Por exemplo, `203.0.113.0/24`.
  - Um intervalo de endereços IPv6, em notação de bloco CIDR. Por exemplo, `2001:db8:1234:1a00::/64`.
  - O ID de uma lista de prefixos. Por exemplo, `pl-1234abc1234abc123`. Para ter mais informações, consulte the section called “Listas de prefixos gerenciados”.
  - O ID de um grupo de segurança. Por exemplo, `sg-1234567890abcdef0`. Para ter mais informações, consulte the section called “Referenciamento de grupo de segurança”.

- (Opcional) Descrição: é possível adicionar uma descrição à regra, que pode ajudá-lo a identificá-la posteriormente. Uma descrição pode ser até 255 caracteres de comprimento. Os caracteres permitidos são a-z, A-Z, 0-9, espaços e ._-:/()#,@[]+=;{}!$*.

Referenciamento de grupo de segurança

Quando você especifica um grupo de segurança como a origem ou o destino de uma regra, a regra afeta todas as instâncias associadas aos grupos de segurança. As instâncias podem se comunicar na direção especificada, usando os endereços IP privados das instâncias, pelo protocolo e pela porta especificados.

O exemplo a seguir representa uma regra de entrada de um grupo de segurança que faz referência ao grupo de segurança sg-0abcdef1234567890. Essa regra permite tráfego SSH de entrada das instâncias associadas a sg-0abcdef1234567890.

Origem	Protocolo	Intervalo de portas
sg-0abcdef1234567890	TCP	22

Ao fazer referência a um grupo de segurança em uma regra de grupo de segurança, observe o seguinte:

- Você pode referenciar um grupo de segurança na regra de entrada de outro grupo de segurança se alguma das seguintes condições for verdadeira:
  - Os grupos de segurança são associados à mesma VPC.
  - Existe uma conexão de emparelhamento entre as VPCs às quais os grupos de segurança são associados.
  - Existe um gateway entre as VPCs às quais os grupos de segurança são associados.
- Você pode referenciar um grupo de segurança na regra de saída de outro grupo de segurança se alguma das seguintes condições for verdadeira:
  - Os grupos de segurança são associados à mesma VPC.
  - Existe uma conexão de emparelhamento entre as VPCs às quais os grupos de segurança são associados.
- Nenhuma regra do grupo de segurança referenciado é adicionada ao grupo de segurança que faz referência a ele.

- Para regras de entrada, as instâncias do EC2 associadas ao grupo de segurança podem receber tráfego de entrada para os endereços IP privados das instâncias do EC2 associadas ao grupo de segurança.
- Para regras de saída, as instâncias do EC2 associadas a um grupo de segurança podem enviar tráfego de saída aos endereços IP privados das instâncias do EC2 associadas ao grupo de segurança referenciado.

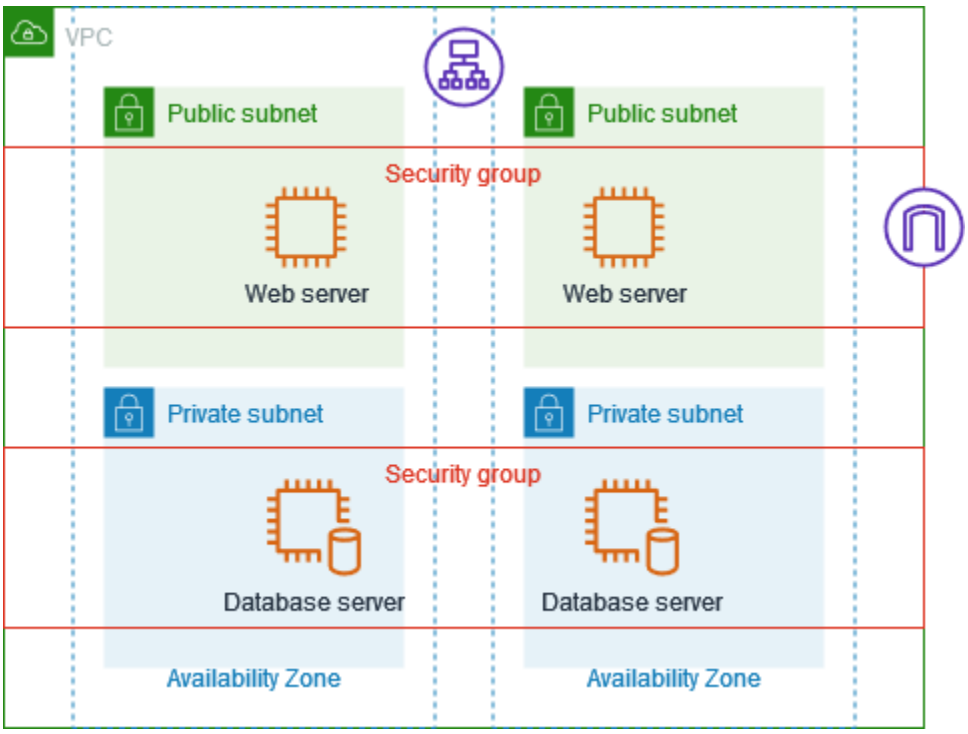
Limitação

Se você configurar rotas para encaminhar o tráfego entre duas instâncias em sub-redes diferentes por meio de um dispositivo middlebox, deverá garantir que os grupos de segurança de ambas as instâncias permitam o fluxo de tráfego entre as instâncias. O grupo de segurança para cada instância deve fazer referência ao endereço IP privado da outra instância ou ao intervalo CIDR da sub-rede que contém a outra instância, como a origem. Se você fizer referência ao grupo de segurança da outra instância como a origem, isso não permitirá que o tráfego flua entre as instâncias.

Exemplo

O diagrama a seguir mostra uma VPC com sub-redes em duas zonas de disponibilidade, um gateway da Internet e um Application Load Balancer. Cada zona de disponibilidade tem uma sub-rede pública para servidores da Web e uma sub-rede privada para servidores de banco de dados. Há grupos de segurança separados para o balanceador de carga, os servidores da Web e os servidores de banco de dados. Crie as seguintes regras de grupos de segurança para permitir o tráfego.

- Adicione regras ao grupo de segurança do balanceador de carga para permitir o tráfego HTTP e HTTPS da Internet. A origem é 0,0.0.0/0.
- Adicione regras ao grupo de segurança dos servidores Web para permitir tráfego HTTP e HTTPS somente do balanceador de carga. A origem é o grupo de segurança do balanceador de carga.
- Adicione regras ao grupo de segurança dos servidores de banco de dados para permitir solicitações de banco de dados dos servidores Web. A origem é o grupo de segurança dos servidores Web.



Tamanho do grupo de segurança

O tipo de origem ou destino determina como cada regra conta para o número máximo de regras que você pode ter por grupo de segurança.

- Uma regra que faz referência a um bloco CIDR é contabilizada como uma regra.
- Uma regra que faz referência a outro grupo de segurança é contabilizada como uma regra, independentemente do tamanho do grupo de segurança referenciado.
- Uma regra que faz referência a uma lista de prefixos gerenciada pelo cliente é contabilizada como o tamanho máximo da lista de prefixos. Por exemplo, se o tamanho máximo da sua lista de prefixos for 20, uma regra que faça referência a essa lista de prefixos será contabilizada como 20 regras.
- Uma regra que utiliza uma lista de prefixos gerenciada por AWS é ponderada pelo peso atribuído a essa lista de prefixos. Por exemplo, se o peso da lista de prefixos for 10, uma regra que faz referência a essa lista será considerada como 10 regras. Para ter mais informações, consulte the section called “Listas de prefixos gerenciados pela AWS disponíveis”.

Regras de grupo de segurança obsoletas

Se a VPC tiver uma conexão de emparelhamento da VPC com outra VPC, ou se utilizar uma VPC compartilhada por outra conta, uma regra do grupo de segurança em sua VPC pode fazer referência a um grupo de segurança no par da VPC ou na VPC compartihada. Isso permite que as instâncias associadas ao grupo de segurança referenciado e aquelas associadas ao grupo de segurança de referência se comuniquem entre si. Para obter mais informações, consulte Atualizar seus grupos de segurança para fazer referência a grupos de segurança de mesmo nível no Guia de emparelhamento da Amazon VPC.

Se você tiver uma regra de grupo de segurança que referencie um grupo de segurança em uma VPC emparelhada, e o grupo de segurança, ou a conexão de emparelhamento da VPC forem excluídos, a regra de grupo de segurança será marcada como obsoleta. Você pode excluir regras de grupo de segurança obsoletas, como faria com qualquer outra regra do grupo de segurança.

Grupo de segurança padrão para VPCs

Suas VPCs padrão e todas as VPCs criadas por você vêm com um grupo de segurança padrão. O nome do grupo de segurança padrão é “default”.

Recomendamos que você crie grupos de segurança para recursos ou grupos de recursos específicos em vez de usar o grupo de segurança padrão. No entanto, se você não associar um grupo de segurança a alguns recursos no momento da criação, nós os associaremos ao grupo de segurança padrão. Por exemplo, se você não especificar um grupo de segurança ao executar uma instância do EC2, associaremos a instância ao grupo de segurança padrão para a VPC.

Noções básicas do grupo de segurança padrão

- Você pode alterar as regras do grupo de segurança padrão.
- Você não pode excluir um grupo de segurança padrão. Se você tentar excluir um grupo de segurança padrão, retornaremos o seguinte código de erro: `Client.CannotDelete`.

Regras padrão

A tabela a seguir descreve as regras de entrada padrão para um grupo de segurança padrão.

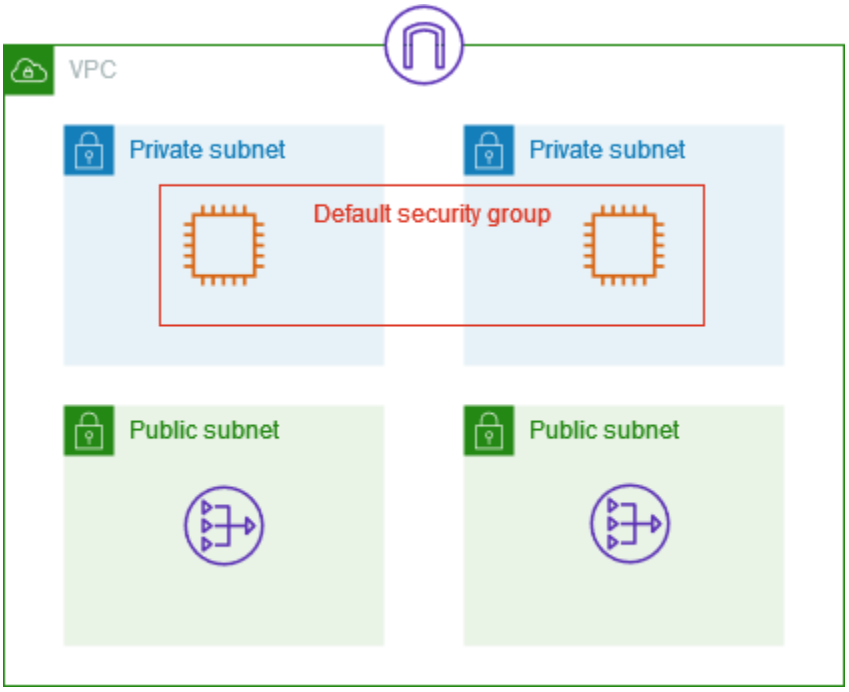
Origem	Protocolo	Intervalo de portas	Descrição
sg-1234567890abcdef0	Todos	Todos	Permite tráfego de entrada de todos os recursos atribuídos a este grupo de segurança. A origem é o ID deste grupo de segurança.

A tabela a seguir descreve as regras de saída padrão para um grupo de segurança padrão.

Destino	Protocolo	Intervalo de portas	Descrição
0.0.0.0/0	Tudo	Tudo	Permite todo o tráfego IPv4 de saída.
::/0	Tudo	Tudo	Permite todo o tráfego IPv6 de saída. Essa regra será adicionad a somente se sua VPC tiver um bloco CIDR IPv6 associado.

Exemplo

O diagrama a seguir mostra uma VPC com um grupo de segurança padrão, um gateway da Internet e um gateway NAT. A segurança padrão contém somente suas regras padrão, e está associada a duas instâncias do EC2 em execução na VPC. Nesse cenário, cada instância pode receber tráfego de entrada da outra instância em todas as portas e protocolos. As regras padrão não permitem que as instâncias recebam tráfego do gateway da Internet ou do gateway NAT. Se as suas instâncias precisarem receber tráfego adicional, recomendamos criar um grupo de segurança com as regras necessárias e associar esse novo grupo de segurança às instâncias em vez de ao grupo de segurança padrão.



Crie um grupo de segurança para a VPC

Sua nuvem privada virtual (VPC) vem com um grupo de segurança padrão. Você pode criar grupos de segurança adicionais. Os grupos de segurança só podem ser usados com os recursos da VPC para a qual foram criados.

Por padrão, novos grupos de segurança começam com apenas uma regra de saída que permite que todo o tráfego deixe as instâncias. Adicione regras para permitir qualquer tráfego de entrada ou para restringir o tráfego de saída. Você pode adicionar regras quando cria um grupo de segurança ou posteriormente. Para ter mais informações, consulte Regras de grupos de segurança.

Permissões obrigatórias

Antes de começar, verifique se você tem as permissões necessárias. Para obter mais informações, consulte:

- Gerenciar grupos de segurança
- Gerenciar regras de grupos de segurança

Para criar um grupo de segurança usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Grupos de segurança.

3. Escolha Create grupo de segurança (Criar grupo de segurança).
4. Insira um nome e uma descrição para o grupo de segurança. Você não pode alterar o nome e a descrição de um grupo de segurança depois que ele foi criado.
5. Para VPC, escolha a VPC na qual você vai criar os recursos aos quais vai associar o grupo de segurança.
6. (Opcional) Para adicionar regras de entrada, escolha Regras de entrada. Para cada regra, escolha Adicionar regra e especifique o protocolo, a porta e a origem. Para ter mais informações, consulte Configurar regras de grupo de segurança.
7. (Opcional) Para adicionar regras de saída, escolha Regras de saída. Em cada regra, escolha Adicionar regra e especifique o protocolo, a porta e o destino.
8. (Opcional) Para adicionar uma tag, escolha Add new tag (Adicionar nova tag) e insira a chave e o valor da tag.
9. Escolha Criar grupo de segurança.

Para criar um grupo de segurança usando o AWS CLI

Use o comando create-security-group.

Ou então, você pode criar um novo grupo de segurança copiando um existente. Quando você copia um grupo de segurança, adicionamos automaticamente as mesmas regras de entrada e saída do grupo de segurança original, e usamos a mesma VPC do grupo de segurança original. Você pode inserir um nome e uma descrição para o novo grupo de segurança. Opcionalmente, você pode escolher uma VPC diferente e modificar as regras de entrada e saída conforme necessário. Mas não pode copiar um grupo de segurança de uma região para outra região.

Para criar um grupo de segurança com base em um já existente

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione um security group.
4. Escolha Ações, Copiar para o novo grupo de segurança.
5. Insira um nome e uma descrição para o grupo de segurança.
6. (Opcional) Escolha outra VPC se necessário.
7. (Opcional) Adicione, remova ou edite as regras de grupo de segurança conforme necessário.
8. Escolha Criar grupo de segurança.

Configurar regras de grupo de segurança

Depois de criar um grupo de segurança, você pode adicionar, atualizar e excluir as regras de grupo de segurança do grupo. Quando você adiciona, atualiza ou exclui uma regra, a alteração é aplicada automaticamente aos recursos associados ao grupo de segurança.

Permissões obrigatórias

Antes de começar, verifique se você tem as permissões necessárias. Para ter mais informações, consulte Gerenciar regras de grupos de segurança.

Origens e destinos

Você pode especificar o seguinte como origens para as regras de entrada ou como destinos para as regras de saída.

- Personalizado: um bloco CIDR IPv4 e um bloco CIDR IPv6, outro grupo de segurança ou uma lista de prefixos.
- Anywhere-IPv4: o bloco CIDR IPv4 0.0.0.0/0.
- Anywhere-IPv6: o bloco CIDR IPv6 ::/0.
- Meu IP: o endereço IPv4 público do computador local.

> **Warning**
>
> Se você escolher Anywhere-IPv4, o tráfego de todos os endereços IPv4 será permitido. Se você escolher Anywhere-IPv6, o tráfego de todos os endereços IPv6 será permitido. É uma prática recomendada autorizar apenas os intervalos de endereços IP específicos que precisam ter acesso a seus recursos.

Para configurar regras de grupo de segurança usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione o grupo de segurança.
4. Para editar as regras de entrada, escolha Editar regras de entrada em Ações ou na guia Regras de entrada.

a. Para adicionar uma regra, escolha Adicionar regra e insira o tipo, o protocolo, a porta e a origem da regra.

   Se o tipo for TCP ou UDP, será necessário inserir o intervalo de portas a ser permitido. Para ICMP personalizado, você deverá escolher o nome do tipo ICMP em Protocol (Protocolo) e, se aplicável, o nome do código em Port range (Intervalo de portas). Para qualquer outro tipo, o protocolo e o intervalo de portas serão configurados para você.

b. Para atualizar uma regra, altere o protocolo, a descrição e a origem da regra, conforme necessário. Porém, você não pode alterar o tipo de origem. Por exemplo, se a origem for um bloco CIDR IPv4, você não poderá especificar um bloco CIDR IPv6, uma lista de prefixos ou um grupo de segurança.

c. Para excluir uma regra, escolha seu botão Excluir.

5. Para editar as regras de saída, escolha Editar regras de saída em Ações ou na guia Regras de saída.

   a. Para adicionar uma regra, escolha Adicionar regra e insira o tipo, o protocolo, a porta e o destino da regra. Você também pode inserir uma descrição opcional.

      Se o tipo for TCP ou UDP, será necessário inserir o intervalo de portas a ser permitido. Para ICMP personalizado, você deverá escolher o nome do tipo ICMP em Protocol (Protocolo) e, se aplicável, o nome do código em Port range (Intervalo de portas). Para qualquer outro tipo, o protocolo e o intervalo de portas serão configurados para você.

   b. Para atualizar uma regra, altere o protocolo, a descrição e a origem da regra, conforme necessário. Porém, você não pode alterar o tipo de origem. Por exemplo, se a origem for um bloco CIDR IPv4, você não poderá especificar um bloco CIDR IPv6, uma lista de prefixos ou um grupo de segurança.

   c. Para excluir uma regra, escolha seu botão Excluir.

6. Selecione Salvar rules.

Para configurar regras de grupo de segurança usando a AWS CLI

- Adicionar: use os comandos authorize-security-group-ingress e authorize-security-group-egress.
- Remover: use os comandos revoke-security-group-ingress e revoke-security-group-egress.
- Modificar: use os comandos modify-security-group-rules, update-security-group-rule-descriptions-ingress e update-security-group-rule-descriptions-egress.

Exclua um grupo de segurança

Quando não precisar mais de um grupo de segurança que você criou, poderá excluí-lo.

Requisitos

- O grupo de segurança não pode estar associado a nenhum recurso.
- O grupo de segurança não pode ser referenciado por nenhuma regra em outro grupo de segurança.
- O grupo de segurança não pode ser o grupo de segurança padrão da VPC.

Para excluir um grupo de segurança usando o console

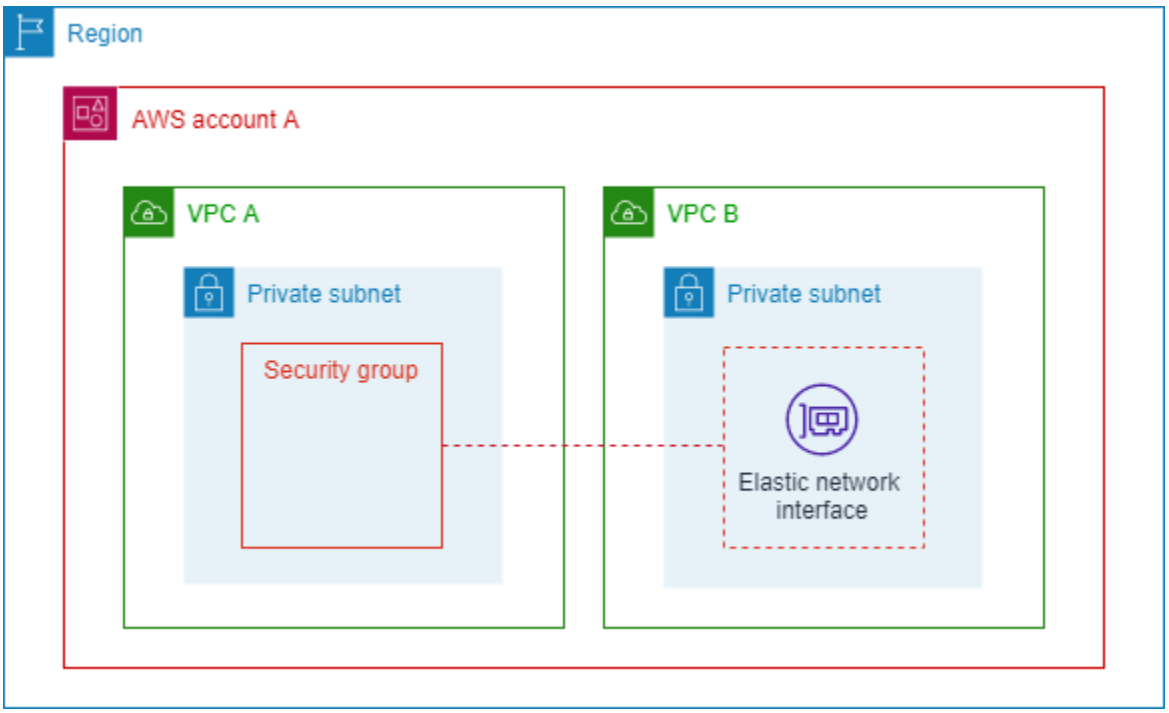
1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione o grupo de segurança e escolha Ações, Excluir grupos de segurança.
4. Caso tenha selecionado mais de um grupo de segurança, será solicitada sua confirmação. Se alguns dos grupos de segurança não puderem ser excluídos, exibiremos o status de cada grupo de segurança, que indicará se ele será ou não excluído. Para confirmar a exclusão, insira Excluir.
5. Escolha Excluir.

Para excluir um grupo de segurança usando a AWS CLI

Use o comando delete-security-group.

Associar grupos de segurança a várias VPCs

Se você tiver workloads em execução em várias VPCs que compartilham requisitos de segurança de rede, poderá usar o atributo Associações de Grupos de Segurança a VPCs para associar um grupo de segurança a várias VPCs na mesma região. Isso permite que você gerencie e mantenha grupos de segurança para várias VPCs em um único local em sua conta.



O diagrama acima mostra a conta A da AWS com duas VPCs. Cada uma das VPCs tem workloads em execução em uma sub-rede privada. Nesse caso, as workloads das sub-redes A e B da VPC compartilham os mesmos requisitos de tráfego de rede, assim, a conta A pode usar o atributo Associações de Grupos de Segurança a VPCs para associar o grupo de segurança da VPC A à VPC B. Todas as atualizações feitas no grupo de segurança associado são aplicadas automaticamente ao tráfego para as workloads na sub-rede da VPC B.

Requisitos do atributo Associações de Grupos de Segurança a VPCs

- Para associar um grupo de segurança à VPC, você deve ser o proprietário da VPC ou uma das sub-redes da VPC deve ser compartilhada com você.
- A VCP e o grupo de segurança devem estar na mesma região da AWS.
- Não é possível associar um grupo de segurança padrão a outra VPC ou associar um grupo de segurança a uma VPC padrão.
- Tanto o proprietário do grupo de segurança quanto o proprietário da VPC podem visualizar as associações do grupo de segurança à VCP.

Serviços compatíveis com esse atributo

- Amazon API Gateway (APIs REST apenas)
- AWS Auto Scaling

- AWS CloudFormation
- Amazon EC2
- Amazon EFS
- Amazon EKS
- Amazon FSx
- AWS PrivateLink
- Amazon Route 53
- Elastic Load Balancing
  - Application Load Balancer
  - Network Load Balancer

Associar um grupo de segurança a outra VPC

Esta seção explica como usar o AWS Management Console e a AWS CLI para associar um grupo de segurança a VPCs.

AWS Management Console

Para associar um grupo de segurança a outra VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação esquerdo, escolha Grupos de segurança.
3. Escolha um grupo de segurança para visualizar os detalhes.
4. Escolha a guia Associações de VPC.
5. Escolha Associate VPC.
6. Em ID da VPC, escolha uma VPC para associar ao grupo de segurança.
7. Escolha Associate VPC.

Command line

Para associar um grupo de segurança a outra VPC

1. Crie uma associação da VPC com associate-security-group-vpc.
2. Verifique o status de uma associação da VPC com describe-security-group-vpc-associations e aguarde até que o status seja `associated`.

A VPC agora está associada ao grupo de segurança.

Depois de associar a VPC ao grupo de segurança, você pode, por exemplo, iniciar uma instância na VPC e escolher esse novo grupo de segurança ou referenciar esse grupo de segurança em uma regra de grupo de segurança existente.

Desassociar um grupo de segurança de outra VPC

Esta seção explica como usar o AWS Management Console e a AWS CLI para desassociar um grupo de segurança de VPCs. Você poderá querer fazer isso se seu objetivo for excluir o grupo de segurança. Grupos de segurança não poderão ser excluídos se estiverem associados. Você só poderá desassociar um grupo de segurança se não houver nenhuma interface de rede na VPC associada que use esse grupo de segurança.

AWS Management Console

Para desassociar um grupo de segurança de uma VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação esquerdo, escolha Grupos de segurança.
3. Escolha um grupo de segurança para visualizar os detalhes.
4. Escolha a guia Associações de VPC.
5. Escolha Desassociar VPC.
6. Em ID da VPC, escolha uma VPC para desassociar do grupo de segurança.
7. Escolha Desassociar VPC.
8. Visualize o Status da dissociação na guia Associações da VPC e aguarde até que o status seja `disassociated`.

Command line

Para desassociar um grupo de segurança de uma VPC

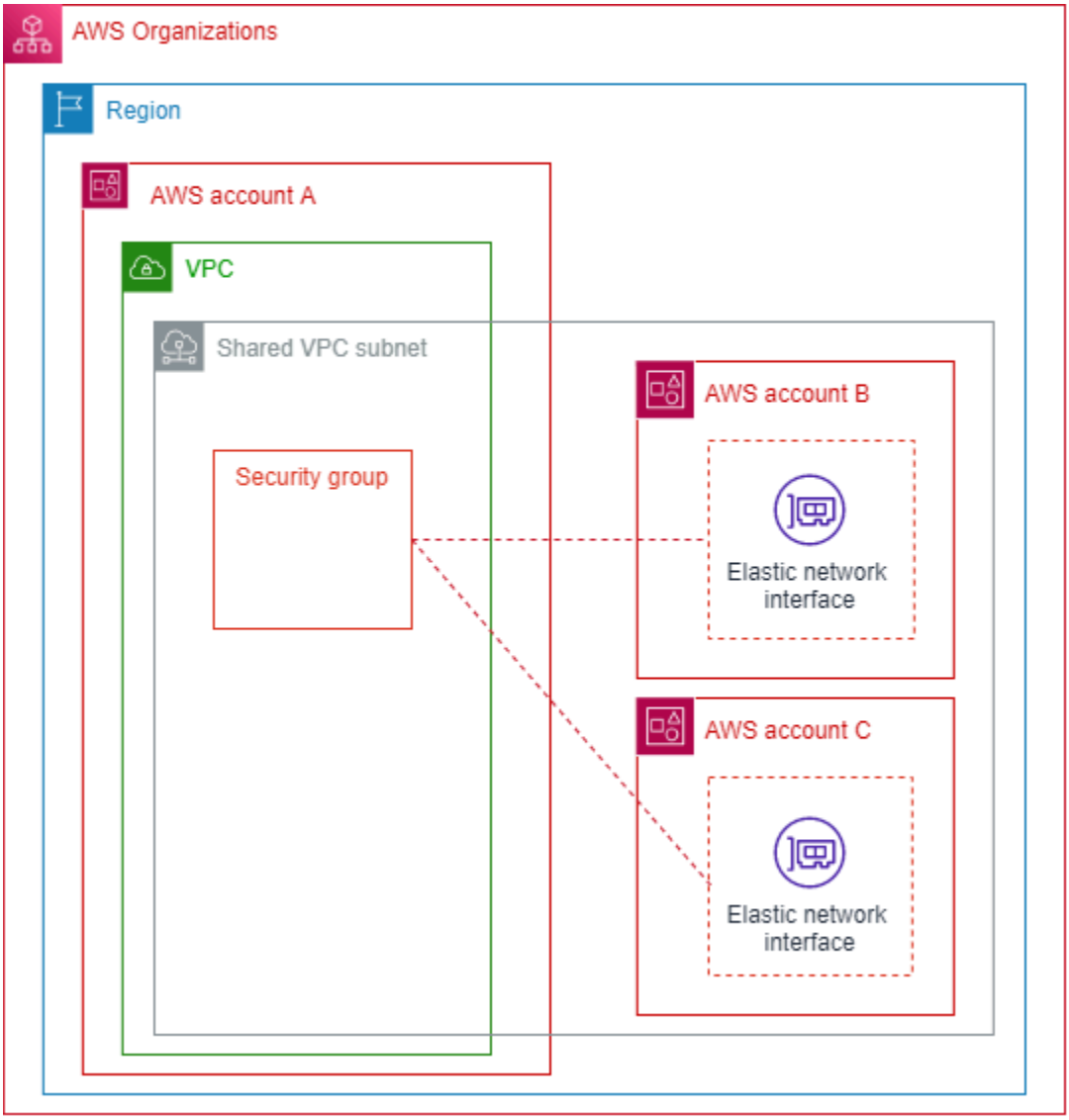
1. Desassocie uma associação da VPC com disassociate-security-group-vpc.
2. Verifique o status de uma desassociação da VPC com describe-security-group-vpc-associations e aguarde até que o status seja `disassociated`.

A VPC agora está desassociada do grupo de segurança.

Compartilhar grupos de segurança com o AWS Organizations

O recurso grupo de segurança compartilhado possibilita compartilhar um grupo de segurança com outras contas do AWS Organizations na mesma região da AWS, tornando o grupo de segurança disponível para ser usado por essas contas.

O diagrama a seguir demonstra como você pode usar o atributo Grupo de Segurança Compartilhado para simplificar o gerenciamento de grupos de segurança entre as contas do AWS Organizations:



Este diagrama mostra três contas que fazem parte da mesma organização. A conta A compartilha uma sub-rede da VPC com as contas B e C. A conta A compartilha o grupo de segurança com as contas B e C usando o atributo Grupo de Segurança Compartilhado. As contas B e C então usam esse grupo de segurança quando iniciam instâncias na sub-rede compartilhada. Isso permite que a

conta A gerencie o grupo de segurança, e todas as atualizações do grupo de segurança se aplicam aos recursos que as contas B e C têm em execução na sub-rede da VPC compartilhada.

Requisitos do atributo Grupo de Segurança Compartilhado

- Esse atributo só está disponível em contas na mesma organização do AWS Organizations. O Compartilhamento de recurso deve estar habilitado no AWS Organizations.
- A conta que compartilha o grupo de segurança deve ser a proprietária da VPC e do grupo de segurança.
- Você não pode compartilhar os grupos de segurança padrão.
- Você não pode compartilhar grupos de segurança que estejam em uma VPC padrão.
- As contas participantes podem criar grupos de segurança em uma VPC compartilhada, mas não podem compartilhar esses grupos de segurança.
- É necessário um conjunto mínimo de permissões para uma entidade principal do IAM compartilhar um grupo de segurança com o AWS RAM. Use as políticas gerenciadas do IAM `AmazonEC2FullAccess` e `AWSResourceAccessManagerFullAccess` para garantir que as entidades superiores do IAM tenham as permissões necessárias para compartilhar e usar os grupos de segurança compartilhados. Se você usar uma política personalizada do IAM, as ações `c2:PutResourcePolicy` e `ec2:DeleteResourcePolicy` serão são necessárias. Essas são ações do IAM realizadas somente com permissão. Se uma entidade principal do IAM não tiver essas permissões, ocorrerá um erro quando ela tentar compartilhar o grupo de segurança usando o AWS RAM.

Serviços compatíveis com esse atributo

- Amazon API Gateway
- Amazon EC2
- Amazon ECS
- Amazon EFS
- Amazon EKS
- Amazon EMR
- Amazon FSx
- Amazon ElastiCache
- AWS Elastic Beanstalk

- AWS Glue
- Amazon MQ
- Amazon SageMaker AI
- Elastic Load Balancing
  - Application Load Balancer
  - Network Load Balancer

Como esse atributo afeta as cotas existentes

Cotas de grupo de segurança se aplicam. No entanto, para a cota “Grupos de segurança por interface de rede”, se um participante usar tanto grupos próprios quanto grupos compartilhados em uma interface de rede elástica (ENI), a cota mínima entre o proprietário e o participante será aplicada.

Exemplo para demonstrar como a cota é afetada por esse atributo:

- Cota da conta do proprietário: 4 grupos de segurança por interface
- Cota da conta do participante: 5 grupos de segurança por interface.
- O proprietário compartilha os grupos SG-O1, SG-O2, SG-O3, SG-O4, SG-O5 com o participante. O participante já tem seus próprios grupos na VPC: SG-P1, SG-P2, SG-P3, SG-P4, SG-P5.
- Se o participante criar uma ENI e usar somente apenas seus próprios grupos, poderá associar todos os 5 grupos de segurança (SG-P1, SG-P2, SG-P3, SG-P4, SG-P5) porque essa é sua cota.
- Se o participante criar uma ENI e usar nela algum grupo compartilhado, poderá associar até 4 grupos. Nesse caso, a cota para essa ENI será o mínimo das cotas do proprietário e do participante. As possíveis configurações válidas serão assim:
  - SG-O1, SG-P1, SG-P2, SG-P3
  - SG-O1, SG-O2, SG-O3, SG-O4

Compartilhar um grupo de segurança

Esta seção explica como usar o AWS Management Console e a AWS CLI para compartilhar um grupo de segurança com outras contas da organização.

AWS Management Console

Para compartilhar um grupo de segurança

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação esquerdo, escolha Grupos de segurança.
3. Escolha um grupo de segurança para visualizar os detalhes.
4. Escolha a guia Sharing (Compartilhamento).
5. Escolha Grupo de segurança compartilhado.
6. Escolha Criar compartilhamento de recursos. Como resultado, o console do AWS RAM será aberto, e nele você criará o compartilhamento de recurso para o grupo de segurança.
7. Insira um Nome para o recurso compartilhado.
8. Em Recursos: opcional, escolha Grupos de segurança.
9. Escolha um grupo de segurança. O grupo de segurança não pode ser um grupo de segurança padrão e não pode estar associado à VPC padrão.
10. Escolha Próximo.
11. Revise as ações que as entidades principais terão permissão de realizar e escolha Avançar.
12. Em Entidades principais: opcional, escolha Permitir compartilhamento apenas dentro da organização.
13. Em Entidades principais, selecione um dos seguintes tipos de entidade principal e insira os números apropriados:

    - Conta da AWS: o número de uma conta da organização.
    - Organização: o ID do AWS Organizations.
    - Unidade organizacional (UO): o ID de uma UO da organização.
    - Perfil do IAM: o ARN de um perfil do IAM. A conta que criou o perfil deve ser membro da mesma organização que a conta que está criando esse compartilhamento de recurso.
    - Usuário do IAM: o ARN de um usuário do IAM. A conta que criou o usuário deve ser membro da mesma organização que a conta que está criando esse compartilhamento de recurso.
    - Entidade principal do serviço: você não pode compartilhar um grupo de segurança com uma entidade principal do serviço.
14. Escolha Adicionar.
15. Escolha Próximo.

16. Escolha Criar compartilhamento de recursos.
17. Em Recursos compartilhados, aguarde para ver o Status de `Associated`. Se houver uma falha na associação do grupo de segurança, a causa talvez seja uma das limitações listadas acima. Visualize os detalhes do grupo de segurança e a guia Compartilhamento na página de detalhes para ver todas as mensagens relacionadas motivo pelo qual um grupo de segurança pode não ser compartilhável.
18. Volte à lista de grupos de segurança no console da VPC.
19. Escolha o grupo de segurança que você compartilhou.
20. Escolha a guia Sharing (Compartilhamento). O recurso do AWS RAM deve estar visível ali. Se não estiver, talvez a criação do recurso compartilhado tenha falhado e seja necessário recriá-la.

Command line

Para compartilhar um grupo de segurança

1. Você primeiro deve criar um compartilhamento de recurso para o grupo de segurança que deseja compartilhar com o AWS RAM. Para ver as etapas de como criar um recurso compartilhado com o AWS RAM usando a AWS CLI, consulte Creating a resource share in AWS RAM no AWS RAM User Guide
2. Para visualizar as associações de compartilhamento de recurso criadas, use get-resource-share-associations.

O grupo de segurança agora está compartilhado. É possível selecionar o grupo de segurança ao iniciar uma instância do EC2 em uma sub-rede compartilhada na mesma VPC.

Parar de compartilhar um grupo de segurança

Esta seção explica como usar o AWS Management Console e a AWS CLI para parar de compartilhar um grupo de segurança com outras contas da organização.

AWS Management Console

Para parar de compartilhar um grupo de segurança

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação esquerdo, escolha Grupos de segurança.

3. Escolha um grupo de segurança para visualizar os detalhes.
4. Escolha a guia Sharing (Compartilhamento).
5. Escolha um compartilhamento de recurso do grupo de segurança e depois Parar de compartilhar.
6. Escolha Sim, parar de compartilhar.

Command line

Para parar de compartilhar um grupo de segurança

Exclua o compartilhamento de recurso com delete-resource-share.

O grupo de segurança não está mais sendo compartilhado. Quando o proprietário deixa de compartilhar um grupo de segurança, as seguintes regras se aplicam:

- As Elastic Network Interfaces (ENIs) de participantes existentes continuam a receber todas as atualizações de regra de grupo de segurança feitas nos grupos de segurança não compartilhados. O cancelamento do compartilhamento só impede que o participante crie novas associações com o grupo não compartilhado.
- Os participantes não podem mais associar o grupo de segurança não compartilhado a suas próprias ENIs.
- Os participantes podem descrever e excluir as ENIs que ainda estão associadas aos grupos de segurança não compartilhados.
- Se os participantes ainda tiverem ENIs associadas ao grupo de segurança não compartilhado, o proprietário não poderá excluir o grupo de segurança não compartilhado. O proprietário só poderá excluir o grupo de segurança depois que os participantes desassociarem (removerem) o grupo de segurança de todas as suas ENIs.
- Os participantes não podem iniciar novas instâncias do EC2 usando uma ENI associada a um grupo de segurança não compartilhado.

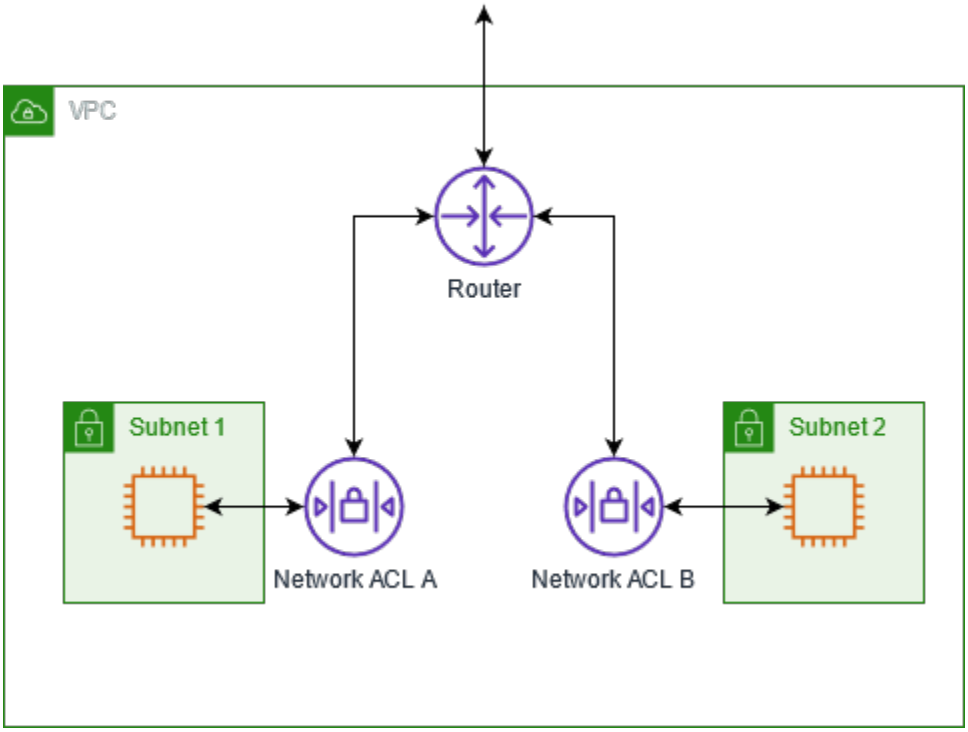
Controlar o tráfego da sub-rede com listas de controle de acesso à rede

Uma lista de controle de acesso (ACL) de rede permite ou não determinado tráfego de entrada ou de saída no nível da sub-rede. Você pode usar a ACL de rede padrão para a VPC ou pode criar uma

ACL de rede personalizada para a VPC com regras semelhantes às regras dos grupos de segurança para adicionar mais uma camada de segurança à VPC.

Não há nenhuma cobrança adicional pelo uso de ACLs de rede.

O diagrama a seguir mostra uma VPC com duas sub-redes. Cada sub-rede tem uma ACL de rede. Quando o tráfego entra na VPC (por exemplo, de uma VPC emparelhada, de uma conexão VPN ou da Internet), o roteador envia o tráfego para seu destino. A ACL da rede A determina qual tráfego destinado à sub-rede 1 tem permissão para entrar na sub-rede 1 e qual tráfego destinado a um local fora da sub-rede 1 tem permissão para sair da sub-rede 1. Da mesma forma, a ACL da rede B determina qual tráfego tem permissão para entrar e sair da sub-rede 2.



Para obter mais informações sobre as diferenças entre grupos de segurança e ACLs de rede, consulte Comparar grupos de segurança e ACLs de rede.

Conteúdo

- Noções básicas de ACL de rede
- Regras de ACL de rede
- ACL de rede padrão para uma VPC
- ACLs de rede personalizadas para sua VPC
- Path MTU Discovery e ACLs de rede

- Criar uma ACL de rede para sua VPC
- Gerenciar associações de ACL de rede para sua VPC
- Excluir uma ACL de rede para sua VPC
- Exemplo: controlar o acesso a instâncias em uma sub-rede

Noções básicas de ACL de rede

Encontram-se a seguir noções essenciais sobre as ACLs de rede:

- Sua VPC possui uma ACL de rede padrão modificável. Por padrão, ela permite todo o tráfego de entrada e saída.
- Você pode criar uma ACL de rede personalizada e associá-la a uma sub-rede para permitir ou recusar tráfego de entrada ou de saída específico por sub-rede.
- Toda sub-rede em sua VPC deve ser associada com uma ACL de rede. Se você não associar explicitamente uma sub-rede com uma ACL de rede, as sub-redes serão associadas automaticamente com a ACL de rede padrão.
- É possível associar uma ACL de rede a várias sub-redes. No entanto, uma sub-rede pode ser associada a apenas uma ACL de rede por vez. Quando uma ACL de rede é associada a uma sub-rede, a associação anterior é removida.
- Uma ACL de rede tem regras de entrada e regras de saída. Cada regra pode permitir ou negar tráfego. Cada regra tem um número de 1 até 32766. Avaliamos as regras na ordem, começando pela regra de número mais baixo, ao decidirmos se o tráfego será permitido ou negado. Se o tráfego corresponder a uma regra, a regra será aplicada e não avaliaremos quaisquer regras adicionais. Para começar, é recomendável criar regras em incrementos (por exemplo, incrementos de 10 ou 100), para que, posteriormente, você possa inserir novas regras, se necessário.
- Avaliamos as regras de ACL da rede quando o tráfego entra e sai da sub-rede, não quando ele é roteado dentro de uma sub-rede.
- Os NACLs são sem estado, o que significa que as informações sobre o tráfego enviado ou recebido anteriormente não são salvas. Se, por exemplo, você criar uma regra de NACL para permitir tráfego de entrada específico para uma sub-rede, as respostas a esse tráfego não serão permitidas automaticamente. Isso contrasta com a forma como os grupos de segurança funcionam. Os grupos de segurança são com estado, o que significa que as informações sobre o tráfego enviado ou recebido anteriormente são salvas. Se, por exemplo, um grupo de segurança permitir tráfego de entrada para uma instância do EC2, as respostas serão permitidas automaticamente, independentemente das regras de saída do grupo de segurança.

- As ACLs de rede não podem bloquear solicitações de DNS de/para o Route 53 Resolver (também conhecido como endereço IP VPC+2 ou AmazonProvidedDNS). Se desejar filtrar solicitações de DNS por meio do Route 53 Resolver, você poderá habilitar o Route 53 Resolver DNS Firewall no Guia do desenvolvedor do Amazon Route 53.
- As ACLs de rede não podem bloquear o Instance Metadata Service (IMDS). Para gerenciar o acesso ao IMDS, consulte Configurar as opções de metadados da instância no Guia do usuário do Amazon EC2.
- As ACLs de rede não filtram tráfego destinado a ou proveniente de:
  - Serviços de nomes de domínio (DNS) da Amazon
  - Dynamic Host Configuration Protocol (DHCP – Protocolo de configuração de host dinâmico) da Amazon
  - Metadados da instância do Amazon EC2
  - Endpoints de metadados de tarefas do Amazon ECS
  - Ativação de licença para instâncias do Windows
  - Serviço de Sincronização Temporal da Amazon
  - Endereços IP reservados usados pelo roteador padrão da VPC
- Há cotas (também conhecidas como limites) para o número de ACLs da rede por VPC e para o número de regras por ACL da rede. Para ter mais informações, consulte Cotas da Amazon VPC.

Regras de ACL de rede

Você pode adicionar ou remover regras de ACL de rede padrão ou criar outras ACLs de rede para sua VPC. Ao adicionar ou remover regras de uma ACL de rede, as alterações são automaticamente aplicadas às sub-redes às quais ela está associada.

Encontram-se a seguir as partes de uma regras de ACL de rede:

- Número da regra. As regras são avaliadas a partir da regra de número mais baixo. Assim que uma regra coincide com o tráfego, ela é aplicada, independentemente de haver qualquer regra com número mais alto que possa contradizê-la.
- Tipo. O tipo de tráfego; por exemplo, SSH. Também é possível especificar todo o tráfego ou um intervalo personalizado.
- Protocol (Protocolo. Você pode especificar qualquer protocolo que tenha um número de protocolo padrão. Para obter mais informações, consulte Protocol Numbers. Se você especificar o ICMP como protocolo, poderá especificar qualquer ou todos os tipos e códigos ICMP.

- Intervalo de portas. A porta de escuta ou o intervalo de portas para o tráfego. Por exemplo, 80 para o tráfego HTTP.
- Source (Origem. [Somente regras de entrada] A fonte do tráfego (intervalo CIDR).
- Destino. [Somente regras de saída] O destino do tráfego (intervalo CIDR).
- Permissão/Negação. Se permite ou nega o tráfego especificado.

Considere os aspectos a seguir ao adicionar e excluir regras de ACL de rede.

Considerações

- Quando você adiciona ou exclui uma regra de uma ACL, todas as sub-redes associadas à ACL ficam sujeitas a essa alteração. As alterações entram em vigor após um curto período.
- Se você adicionar uma regra usando uma ferramenta de linha de comando ou a API do Amazon EC2, o intervalo CIDR será modificado automaticamente para sua forma canônica. Por exemplo, se você especificar `100.68.0.18/18` para o intervalo CIDR, criaremos uma regra com um intervalo CIDR `100.68.0.0/18`.
- Recomenda-se adicionar uma regra de negação em uma situação em que é realmente necessário abrir um amplo intervalo de portas, mas existem determinadas portas nesse intervalo às quais o acesso deve ser negado. Certifique-se de atribuir à regra de negação um número menor do que a regra que permite o tráfego em um intervalo mais amplo de portas.
- Se você adicionar e excluir regras de uma ACL de rede ao mesmo tempo, tenha cuidado. Se você excluir regras de entrada ou saída e, em seguida, adicionar mais entradas novas do que o permitido (consulte Cotas da Amazon VPC), as entradas selecionadas para exclusão serão removidas e novas entradas não serão adicionadas. Isso poderá causar problemas de conectividade inesperados e impedir o acesso a sua VPC.

ACL de rede padrão para uma VPC

Sua nuvem privada virtual (VPC) vem automaticamente com uma ACL de rede padrão. Uma ACL de rede padrão é configurada para permitir todo o tráfego de entrada e saída das sub-redes às quais está associada. Além disso, toda ACL de rede contém regras cujo número é um asterisco (*). Essas regras garantem que, se um pacote não corresponder a nenhuma das outras regras numeradas, o acesso será negado.

É possível modificar uma ACL de rede padrão adicionando regras ou removendo as regras numeradas padrão. Não é possível excluir uma regra cujo número é um asterisco.

Regras de entrada padrão

A tabela a seguir mostra as regras de entrada padrão para uma ACL de rede padrão. As regras para IPv6 serão adicionadas somente se você criar a VPC com um bloco CIDR IPv6 associado ou se associar um bloco CIDR IPv6 à VPC. No entanto, se você tiver modificado as regras de entrada de uma ACL de rede padrão, não adicionaremos automaticamente uma regra para permitir todo o tráfego IPv6 de entrada quando você associar um bloco IPv6 à VPC.

Nº da regra	Type	Protocolo	Intervalo de portas	Origem	Permissão/ Negação
100	Todo tráfego IPv4	Todos	Tudo	0.0.0.0/0	PERMISSÃO
101	Todo tráfego IPv6	Tudo	Tudo	::/0	PERMISSÃO
*	Todo o tráfego	Tudo	Tudo	0.0.0.0/0	DENY
*	Todo tráfego IPv6	Tudo	Tudo	::/0	DENY

Regras de saída padrão

A tabela a seguir mostra as regras de saída padrão para uma ACL de rede padrão. As regras para IPv6 serão adicionadas somente se você criar a VPC com um bloco CIDR IPv6 associado ou se associar um bloco CIDR IPv6 à VPC. No entanto, se você tiver modificado as regras de saída de uma Network ACL padrão, não adicionaremos a regra que permite todo o tráfego IPv6 de saída quando você associar um bloco IPv6 à VPC.

Nº da regra	Type	Protocolo	Intervalo de portas	Destino	Permissão/ Negação
100	Todo o tráfego	Tudo	Tudo	0.0.0.0/0	PERMISSÃO

Nº da regra	Type	Protocolo	Intervalo de portas	Destino	Permissão/ Negação
101	Todo tráfego IPv6	Tudo	Tudo	::/0	PERMISSÃO
*	Todo o tráfego	Tudo	Tudo	0.0.0.0/0	DENY
*	Todo tráfego IPv6	Tudo	Tudo	::/0	DENY

ACLs de rede personalizadas para sua VPC

Você pode criar uma ACL de rede personalizada e associá-la a uma sub-rede para permitir ou recusar tráfego de entrada ou de saída específico por sub-rede. Para ter mais informações, consulte the section called “Criar uma ACL de rede”.

Toda ACL de rede contém uma regra de entrada padrão e uma regra de saída padrão cujo número é um asterisco (*). Essas regras garantem que, se um pacote não corresponder a nenhuma das outras regras, o acesso será negado.

É possível modificar uma ACL de rede adicionando ou removendo regras. Não é possível excluir uma regra cujo número é um asterisco.

Para cada regra adicionada, deve haver uma regra de entrada ou de saída que permita o tráfego de resposta. Para obter mais informações sobre como selecionar o intervalo de portas efêmero apropriado, consulte Portas efêmeras.

Exemplo de regras de entrada

A tabela a seguir mostra exemplos de regras de entrada para uma ACL de rede. As regras para IPv6 serão adicionadas somente se a VPC tiver um bloco CIDR IPv6 associado. Os tráfegos IPv4 e IPv6 são avaliados separadamente. Portanto, nenhuma das regras para tráfego IPv4 se aplicam a tráfego IPv6. É possível adicionar regras de IPv6 ao lado das regras de IPv4 correspondentes ou adicionar as regras de IPv6 após a última regra de IPv4.

Quando um pacote chega à sub-rede, nós o avaliamos em relação às regras de entrada da ACL de rede associada à sub-rede, começando pela regra de menor numeração. Por exemplo, suponha que

haja tráfego IPv4 destinado à porta HTTPS (443). O pacote não corresponde à regra 100 ou 105. Ele corresponde à regra 110, que permite o tráfego na sub-rede. Se o pacote tivesse sido destinado à porta 139 (NetBIOS), ele não corresponderia a nenhuma das regras numeradas, então a regra * para tráfego IPv4 negaria o pacote.

Nº da regra	Type	Protocolo	Intervalo de portas	Origem	Permissão /Negação	Comentários
100	HTTP	TCP	80	0.0.0.0/0	PERMISSÃ	Permite tráfego HTTP de entrada de qualquer endereço IPv4.
105	HTTP	TCP	80	::/0	PERMISSÃ	Permite tráfego HTTP de entrada de qualquer endereço IPv6.
110	HTTPS	TCP	443	0.0.0.0/0	PERMISSÃ	Permite tráfego HTTPS de entrada de qualquer endereço IPv4.
115	HTTPS	TCP	443	::/0	PERMISSÃ	Permite tráfego HTTPS de entrada de qualquer endereço IPv6.
120	SSH	TCP	22	*192.0.2.0 /24*	PERMISSÃ	Permite tráfego SSH de entrada de um intervalo de endereços IPv4 públicos de sua rede doméstica (no gateway da Internet).

Nº da regra	Type	Protocolo	Intervalo de portas	Origem	Permissão /Negação	Comentários
140	TCP personalizado	TCP	32768-65535	0.0.0.0/0	PERMISSÃ	Permite tráfego IPv4 de retorno de entrada da Internet (para solicitações originadas na sub-rede).
145	TCP personalizado	TCP	32768-65535	::/0	PERMISSÃ	Permite tráfego IPv6 de retorno de entrada da Internet (para solicitações originadas na sub-rede).
*	Todo o tráfego	Tudo	Tudo	0.0.0.0/0	NEGAÇÃO	Nega todos os tráfegos IPv4 de entrada ainda não controlados por uma regra precedente (não modificável).
*	Todo o tráfego	Tudo	Tudo	::/0	NEGAÇÃO	Nega todos os tráfegos IPv6 de entrada ainda não controlados por uma regra precedente (não modificável).

Exemplo de regras de saída

A tabela a seguir mostra exemplos de regras de saída para uma ACL de rede personalizada. As regras para IPv6 serão adicionadas somente se a VPC tiver um bloco CIDR IPv6 associado. Os tráfegos IPv4 e IPv6 são avaliados separadamente. Portanto, nenhuma das regras para tráfego IPv4 se aplicam a tráfego IPv6. É possível adicionar regras de IPv6 ao lado das regras de IPv4 correspondentes ou adicionar as regras de IPv6 após a última regra de IPv4.

Nº da regra	Type	Protocolo	Intervalo de portas	Destino	Permissão /Negação	Comentários
100	HTTP	TCP	80	0.0.0.0/0	PERMISSÃ	Permite tráfego HTTP IPv4 de saída da sub-rede para a Internet.
105	HTTP	TCP	80	::/0	PERMISSÃ	Permite tráfego HTTP IPv6 de saída da sub-rede para a Internet.
110	HTTPS	TCP	443	0.0.0.0/0	PERMISSÃ	Permite tráfego HTTPS IPv4 de saída da sub-rede para a Internet.
115	HTTPS	TCP	443	::/0	PERMISSÃ	Permite tráfego HTTPS IPv6 de saída da sub-rede para a Internet.
120	TCP personalizado	TCP	*1024-655 5*	*192.0.2.(/24*	PERMISSÃ	Permite respostas de saída para tráfego SSH proveniente da rede interna.
140	TCP personalizado	TCP	*32768-65 35*	0.0.0.0/0	PERMISSÃ	Permite respostas IPv4 de saída a clientes na Internet (por exemplo, fornecimento de páginas da Web).
145	TCP personalizado	TCP	*32768-65 35*	::/0	PERMISSÃ	Permite respostas IPv6 de saída a clientes na Internet (por exemplo,

Nº da regra	Type	Protocolo	Intervalo de portas	Destino	Permissão /Negação	Comentários
						fornecimento de páginas da Web).
*	Todo o tráfego	Tudo	Tudo	0.0.0.0/0	DENY	Nega todos os tráfegos IPv4 de saída ainda não controlados por uma regra precedente.
*	Todo o tráfego	Tudo	Tudo	::/0	DENY	Nega todos os tráfegos IPv6 de saída ainda não controlados por uma regra precedente.

Portas efêmeras

A ACL de rede de exemplo na seção precedente usa o intervalo de portas efêmero 32768-65535. Entretanto, é recomendável usar um intervalo diferente para suas ACLs de rede dependendo do tipo de cliente que você estiver usando ou com o qual estiver se comunicando.

O cliente que inicia a solicitação escolhe o intervalo de portas efêmero. O intervalo varia dependendo do sistema operacional do cliente.

- Muitos kernels Linux (incluindo o kernel Amazon Linux) usam portas 32768-61000.
- As solicitações originadas do Elastic Load Balancing usam as portas 1024-65535.
- Os sistemas operacionais Windows até o Windows Server 2003 usam portas 1025-5000.
- O Windows Server 2008 e versões posteriores usam portas 49152-65535.
- Um gateway NAT usa as portas 1024 a 65535.
- As funções do AWS Lambda usam portas 1024-65535.

Por exemplo, se uma solicitação chegar ao servidor da web em sua VPC de um cliente Windows 10 na Internet, sua ACL de rede precisará de uma regra de saída para permitir o tráfego destinado às portas 49152 a 65535.

Se uma instância em sua VPC for o cliente que está iniciando uma solicitação, sua ACL de rede precisará de uma regra de entrada para permitir o tráfego destinado às portas efêmeras específicas do sistema operacional da instância.

Na prática, para abranger os diferentes tipos de cliente que podem iniciar tráfego para instâncias voltadas para o público em sua VPC, você pode abrir as portas efêmeras 1024 a 65535. Entretanto, você pode também adicionar regras à ACL para negar tráfego a qualquer porta mal-intencionado dentro do intervalo. Não se esqueça de inserir regras de negação na tabela antes de inserir regras de permissão que abram um amplo intervalo de portas efêmeras.

ACLs de rede personalizadas e outros serviços da AWS

Se você criar uma ACL de rede, esteja ciente de como ela pode afetar os recursos que você criar usando outros serviços de AWS.

Com o Elastic Load Balancing, se a sub-rede das instâncias de backend tiver uma ACL de rede à qual você tenha adicionado uma regra de negação para todo o tráfego com uma origem de `0.0.0.0/0` ou CIDR da sub-rede, o balanceador de carga não conseguirá realizar verificações de integridade nas instâncias. Para obter mais informações sobre as regras recomendadas de ACL da rede para seus balanceadores de carga e instâncias de backend, consulte o seguinte:

- ACLs da rede para o Application Load Balancer
- ACLs da rede para o Network Load Balancer
- ACLs da rede para o Classic Load Balancer

Solucionar problemas de acessibilidade

O Reachability Analyzer é uma ferramenta de análise de configuração estática. Use o Reachability Analyzer para analisar e depurar a acessibilidade da rede entre dois recursos em sua VPC. O Reachability Analyzer produz detalhes salto a salto do caminho virtual entre esses recursos quando eles estão acessíveis e identifica o componente responsável pelo bloqueio quando eles estão inacessíveis. Por exemplo, ele pode identificar regras de ACL de rede ausentes ou mal configuradas.

Para obter mais informações, consulte o Guia do Analisador de Acessabilidade.

Path MTU Discovery e ACLs de rede

O Path MTU Discovery é usado para determinar o MTU do caminho entre dois dispositivos. A MTU do caminho é o tamanho de pacote máximo suportado no caminho entre o host de origem e o host de recepção.

Para o IPv4, quando um host enviar um pacote que for maior que a MTU do host de recebimento ou que a MTU de um dispositivo ao longo do caminho, o host ou o dispositivo de recebimento eliminará o pacote e retornará a seguinte mensagem ICMP: `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` (Tipo 3, Código 4). Isso instrui o host de transmissão a dividir a carga útil em vários pacotes menores e, em seguida, retransmiti-los.

O protocolo IPv6 não é compatível com a fragmentação na rede. Se um host enviar um pacote que for maior que a MTU do host de recebimento ou que a MTU de um dispositivo ao longo do caminho, o host ou dispositivo de recebimento eliminará o pacote e retornará a seguinte mensagem ICMP: `ICMPv6 Packet Too Big (PTB)` (Tipo 2). Isso instrui o host de transmissão a dividir a carga útil em vários pacotes menores e, em seguida, retransmiti-los.

Se a maximum transmission unit (MTU – unidade máxima de transmissão) entre hosts nas sub-redes for diferente, ou suas instâncias se comunicam com pares pela Internet, será necessário adicionar a regra de ACL de rede a seguir, tanto de entrada como de saída. Isso garante que a Path MTU Discovery funcione corretamente e evite a perda de pacotes. Selecione Custom ICMP Rule (Regra ICMP personalizada) para o tipo e Destination Unreachable (Destino inacessível), fragmentation required, and DF flag set (fragmentação necessária e sinalizador DF definido) para o intervalo de portas (tipo 3, código 4). Se você usar o rastreamento de rotas, adicione também a seguinte regra: selecione Custom ICMP Rule (Regra personalizada de ICMP) para o tipo e Time Exceeded (Tempo excedido), TTL expired transit (Trânsito de TTL expirado) para o intervalo de porta (tipo 11, código 0). Para obter mais informações, consulte Unidade de transmissão máxima (MTU) de rede para a instância do EC2 no Guia do usuário do Amazon EC2.

Criar uma ACL de rede para sua VPC

As tarefas a seguir mostram como criar uma ACL de rede, adicionar regras à ACL de rede e, em seguida, associar a ACL de rede a uma sub-rede.

Tarefas

- Etapa 1. Criar uma ACL de rede
- Etapa 2. Adicionar regras

- Etapa 3. Associar uma sub-rede a uma ACL de rede
- (Opcional) Gerenciar ACLs de rede usando o Firewall Manager

Etapa 1. Criar uma ACL de rede

Você pode criar uma ACL de rede personalizada para sua VPC. As regras iniciais de uma ACL de rede personalizada bloqueiam todo o tráfego de entrada e saída. Sua nova ACL de rede personalizada não está associada a uma sub-rede por padrão e deve ser associada explicitamente a sub-redes.

Para criar uma ACL de rede usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Network ACLs.
3. Escolha Criar ACL de rede.
4. (Opcional) Em Nome, insira um nome para a sua ACL de rede.
5. Em VPC, selecione a VPC.
6. (Opcional) Em Tags, escolha Adicionar tag e insira uma chave de tag e um valor de tag.
7. Escolha Criar ACL de rede.

Para criar uma ACL de rede usando a linha de comando

- create-network-acl (AWS CLI)
- New-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Etapa 2. Adicionar regras

É possível adicionar regras que permitam ou neguem tráfego de entrada ou saída.

Processamos as regras sequencialmente, começando pela regra com o número mais baixo. É recomendável deixar lacunas entre os números de regra (como 100, 200, 300), em vez de usar números sequenciais (101, 102, 103). Desse modo, fica mais fácil adicionar uma nova regra sem precisar renumerar as regras existentes.

Se você estiver usando a API do Amazon EC2 ou uma ferramenta de linha de comando, não será possível modificar regras. Só é possível adicionar e excluir regras. Se você estiver usando o console

da Amazon VPC, poderá modificar as entradas das regras existentes. O console remove a regra existente e adiciona uma nova regra para você. Se você precisar mudar a ordem de uma regra na ACL, precisará adicionar uma nova regra com o novo número e depois excluir a regra original.

Para adicionar regras a uma ACL de rede usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Network ACLs.
3. Selecione a ACL de rede.
4. Para adicionar uma regra de entrada, faça o seguinte:
   a. Escolha a guia Regras de entrada.
   b. Na página Editar regras de entrada, escolha Adicionar nova regra.
   c. Insira um número de regra que ainda não esteja em uso, um tipo, protocolo, intervalo de portas, origem e se deseja permitir ou negar o tráfego. Para alguns tipos, preenchemos o protocolo e a porta para você. Se você for solicitado a inserir um intervalo de portas, insira um número de porta ou um intervalo de portas (por exemplo, 49152-65535).

      Para usar um protocolo que não está listado, escolha Protocolo personalizado para o tipo e, em seguida, selecione o protocolo. Para obter mais informações, consulte Números de protocolos IANA.
   d. Escolha Salvar alterações.
5. Para adicionar uma regra de saída, faça o seguinte:
   a. Escolha a guia Outbound rules (Regras de saída).
   b. Selecione Editar regras de saída, Adicionar nova regra.
   c. Insira um número de regra que ainda não esteja em uso, um tipo, protocolo, intervalo de portas, origem e se deseja permitir ou negar o tráfego. Para alguns tipos, preenchemos o protocolo e a porta para você. Se você for solicitado a inserir um intervalo de portas, insira um número de porta ou um intervalo de portas (por exemplo, 49152-65535).

      Para usar um protocolo que não está listado, escolha Protocolo personalizado para o tipo e, em seguida, selecione o protocolo. Para obter mais informações, consulte Números de protocolos IANA.
   d. Escolha Salvar alterações.

Para adicionar uma regra a uma ACL de rede usando a linha de comando

- create-network-acl-entry (AWS CLI)
- New-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Para substituir uma regra em uma ACL de rede usando a linha de comando

- replace-network-acl-entry (AWS CLI)
- Set-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Para excluir uma regra de uma ACL de rede usando a linha de comando

- delete-network-acl-entry (AWS CLI)
- Remove-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Etapa 3. Associar uma sub-rede a uma ACL de rede

Para aplicar as regras de uma ACL de rede a uma sub-rede específica, você deve associar a sub-rede a uma ACL de rede. É possível associar uma ACL de rede a várias sub-redes. No entanto, uma sub-rede pode ser associada a apenas uma ACL de rede. Por padrão, as sub-redes não associadas a uma ACL específica são associadas à ACL de rede padrão.

Para associar uma sub-rede a uma ACL de rede

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Network ACLs e depois selecione a Network ACL.
3. No painel de detalhes, na guia Subnet Associations, escolha Edit. Marque a caixa de seleção Associar para a sub-rede associada à ACL de rede e escolha Salvar.

(Opcional) Gerenciar ACLs de rede usando o Firewall Manager

O AWS Firewall Manager simplifica as tarefas de administração e manutenção de ACLs de rede entre várias contas e sub-redes. Você pode usar o Firewall Manager para monitorar contas e sub-redes da sua organização e aplicar automaticamente as configurações de ACL de rede que definiu. O Firewall Manager é especialmente útil quando você deseja proteger toda a organização ou

quando adiciona frequentemente, de uma conta de administrador central, novos recursos que deseja proteger automaticamente.

Com uma política de ACL de rede do Firewall Manager, usando uma única conta de administrador, você pode configurar, monitorar e gerenciar os conjuntos mínimos de regras que deseja definir nas ACLs de rede usadas em toda a sua organização. Você especifica quais contas e sub-redes da organização estão no escopo da política do Firewall Manager. O Firewall Manager relata o status de conformidade das ACLs de rede para as sub-redes dentro do escopo, e o Firewall Manager pode ser configurado para automatizar a correção de ACLs de rede fora de conformidade.

Para obter mais informações, consulte os seguintes recursos no Guia do desenvolvedor do AWS Firewall Manager:

- Pré-requisitos do AWS Firewall Manager
- Configurar as políticas de ACL de rede do AWS Firewall Manager
- Como usar políticas de ACL de rede com o Firewall Manager

Gerenciar associações de ACL de rede para sua VPC

Cada sub-rede é associada a uma ACL de rede. Quando você cria uma sub-rede pela primeira vez, ela é associada à ACL de rede padrão para a VPC. Você pode criar uma ACL de rede personalizada e associá-la a uma ou mais sub-redes, substituindo a associação de ACL de rede anterior.

Tarefas

- Descrever suas associações de ACL de rede
- Alterar as sub-redes associadas a uma ACL de rede
- Alterar a ACL de rede associada a uma sub-rede

Descrever suas associações de ACL de rede

É possível descrever a ACL de rede associada a uma sub-rede e também descrever quais sub-redes estão associadas a uma ACL de rede.

Para descrever a ACL de rede associada a uma sub-rede usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Sub-redes.

3. Selecione a sub-rede.
4. Selecione a guia ACL de rede.

Para descrever a ACL de rede associada a uma sub-rede usando a AWS CLI

Use o comando describe-network-acls a seguir para listar a ACL de rede associada à sub-rede especificada.

```
aws ec2 describe-network-acls --filters Name=association.subnet-
id,Values=subnet-0d2d1b81e0bc9c6d4 --query NetworkAcls[*].NetworkAclId
```

O seguinte é um exemplo de saída.

```
[
    "acl-03701d1f82d8c3fd6"
]
```

Para descrever as sub-redes associadas a uma ACL de rede usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Network ACLs.
3. Selecione a ACL de rede.
4. Selecione a guia Associações de sub-rede.

Para descrever as sub-redes associadas a uma ACL de rede usando o AWS CLI

Use o comando describe-network-acls a seguir para listar as sub-redes associadas à ACL de rede especificada.

```
aws ec2 describe-network-acls --network-acl-ids acl-060415a18fcc9afde --query
 NetworkAcls[*].Associations[].SubnetId
```

O seguinte é um exemplo de saída.

```
[
    "subnet-0d2d1b81e0bc9c6d4",
    "subnet-0e990c67809773b19",
    "subnet-0eb17d85f5dfd33b1",
```

```
    "subnet-0e01d500780bb7468"
]
```

Alterar as sub-redes associadas a uma ACL de rede

É possível desassociar uma ACL de rede personalizada de uma sub-rede. Após você desassociar uma sub-rede de uma ACL de rede personalizada, nós a associamos automaticamente à ACL de rede padrão para a VPC. As alterações entrarão em vigor após um curto período.

Para alterar as sub-redes associadas a uma ACL de rede

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Network ACLs.
3. Selecione a ACL de rede.
4. Escolha Ações, Editar associações de sub-redes.
5. Remova a sub-rede de Sub-redes selecionadas.
6. Escolha Salvar alterações.

Alterar a ACL de rede associada a uma sub-rede

Você pode mudar a ACL de rede que está associada a uma sub-rede. Por exemplo, quando você cria uma sub-rede, ela é inicialmente associada à ACL de rede padrão da VPC. Se você criar uma ACL de rede personalizada, aplique as regras da ACL de rede associando a ACL de rede a uma ou mais sub-redes.

Depois de alterar a ACL de rede de uma sub-rede, as alterações entrarão em vigor após um curto período.

Para alterar a ACL de rede associada a uma sub-rede

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Sub-redes.
3. Selecione a sub-rede.
4. Escolha Ações, Editar associação de ACL de rede.
5. Em ID da ACL de rede, selecione a ACL de rede a ser associada à sub-rede e revise as regras de entrada e saída da ACL de rede selecionada.
6. Escolha Salvar.

Para substituir uma associação de ACL de rede usando a linha de comando

- replace-network-acl-association (AWS CLI)
- Set-EC2NetworkAclAssociation (AWS Tools for Windows PowerShell)

Excluir uma ACL de rede para sua VPC

Quando não precisar mais de uma ACL de rede, você poderá excluí-la. Não é possível excluir uma ACL de rede quando há sub-redes associadas a ela. Não é possível excluir a ACL de rede padrão.

Para remover associações de sub-rede de uma ACL de rede usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Network ACLs. A coluna Associadas a indica o número de sub-redes associadas a cada ACL de rede. Essa coluna será - se não houver sub-redes associadas.
3. Selecione a ACL de rede.
4. Escolha Ações, Editar associações de sub-redes.
5. Remova as associações de sub-rede.
6. Escolha Salvar alterações.

Para descrever suas ACLs de rede, incluindo associações, usando a linha de comando

- describe-network-acls (AWS CLI)
- Get-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Para substituir uma associação de ACL de rede usando a linha de comando

- replace-network-acl-association (AWS CLI)
- Set-EC2NetworkAclAssociation (AWS Tools for Windows PowerShell)

Para excluir uma ACL de rede usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Network ACLs.

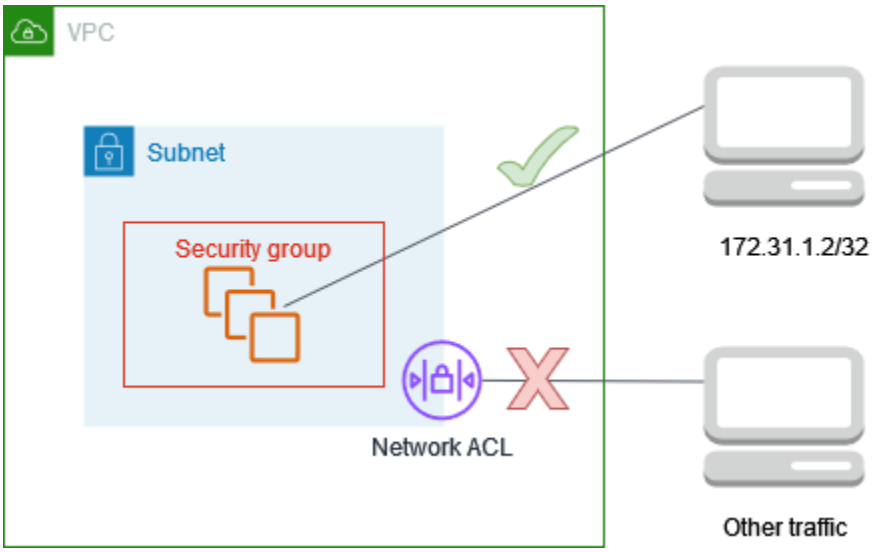
3. Selecione a ACL de rede.
4. Escolha Ações, Excluir ACLs de rede.
5. Quando a confirmação for solicitada, insira **`delete`** e selecione Excluir.

Para excluir uma ACL de rede usando a linha de comando

- delete-network-acl (AWS CLI)
- Remove-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Exemplo: controlar o acesso a instâncias em uma sub-rede

Neste exemplo, as instâncias na sub-rede podem se comunicar umas com as outras e são acessíveis de um computador remoto confiável para a realização de tarefas administrativas. O computador remoto pode ser um computador em sua rede local, conforme mostrado no diagrama, ou uma instância em uma sub-rede ou VPC diferente. As regras de ACL de rede para a sub-rede e as regras do grupo de segurança para as instâncias permitem o acesso desde o endereço IP do seu computador remoto. Todo o outros tráfego proveniente da Internet ou de outras redes é negado.



Usar uma ACL de rede oferece a flexibilidade de alterar os grupos de segurança ou as regras de grupos de segurança para suas instâncias, ao mesmo tempo em que conta com a ACL de rede como uma camada de defesa de backup. Por exemplo, se você atualizar acidentalmente o grupo de segurança para permitir acesso SSH de entrada de qualquer lugar, mas a ACL de rede permitir acesso somente a partir do intervalo de endereços IP do computador remoto, então a ACL de rede negará tráfego SSH de entrada de quaisquer outros endereços IP.

Regras de ACL de rede

A seguir estão exemplos de regras de entrada para a ACL de rede associada à sub-rede. Essas regras se aplicam a todas as instâncias na sub-rede.

Nº da regra	Type	Protocolo	Intervalo de portas	Origem	Permissão/ Negação	Comentários
100	SSH	TCP	22	*172.31.1.2/32*	PERMISSÃO	Permitir tráfego de entrada do computador remoto.
*	Todo o tráfego	Tudo	Tudo	0.0.0.0/0	DENY	Negar todos os outros tráfegos de entrada.

A seguir estão exemplos de regras de saída para a ACL de rede associada à sub-rede. ACLs de rede são stateless. Portanto, é necessário incluir uma regra que permita respostas ao tráfego de entrada.

Nº da regra	Type	Protocolo	Intervalo de portas	Destino	Permissão/ Negação	Comentários
100	TCP personalizado	TCP	1024-65535	*172.31.1.2/32*	PERMISSÃO	Permite respostas de saída ao computador remoto.
*	Todo o tráfego	Tudo	Tudo	0.0.0.0/0	NEGAÇÃO	Nega todos os outros

Nº da regra	Type	Protocolo	Intervalo de portas	Destino	Permissão/ Negação	Comentários
						tráfegos de saída.

Regras de grupos de segurança

A seguir estão exemplos de regras de entrada para o grupo de segurança associado às instâncias. Essas regras se aplicam a todas as instâncias associadas ao grupo de segurança. Um usuário com a chave privada do par de chaves associado às instâncias pode se conectar às instâncias a partir do computador remoto via SSH.

Tipo de protocolo	Protocolo	Intervalo de portas	Origem	Comentários
Todo o tráfego	Tudo	Tudo	*sg-1234567890abcdef0*	Permitir comunicação entre as instâncias associadas a este grupo de segurança.
SSH	TCP	22	*172.31.1.2/32*	Permitir acesso SSH de entrada do computador remoto.

A seguir estão exemplos de regras de saída para o grupo de segurança associado às instâncias. Os grupos de segurança são com estado. Portanto, você não precisa de uma regra que permita respostas ao tráfego de entrada.

Tipo de protocolo	Protocolo	Intervalo de portas	Destino	Comentários
Todo o tráfego	Tudo	Tudo	*sg-1234567890abcdef0*	Permitir comunicação entre as instâncias associadas a este grupo de segurança.

Resiliência na Amazon Virtual Private Cloud

A infraestrutura global da AWS baseia-se em Regiões da AWS e em zonas de disponibilidade. A Regiões da AWS oferece várias zonas de disponibilidade separadas e isoladas fisicamente que são conectadas com baixa latência, altas taxas de throughput e em redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data centers tradicionais.

As Regiões da AWS são os principais blocos de construção, cada uma representando uma localização geográfica distinta que abriga várias zonas de disponibilidade separadas e isoladas fisicamente. Essas zonas de disponibilidade são conectadas com baixa latência, throughput elevado e estruturas de rede altamente redundantes, permitindo comunicação e transferência de dados sem interrupções entre elas.

A arquitetura das zonas de disponibilidade é um diferencial importante, pois elas foram projetadas para serem muito mais robustas e tolerantes a falhas do que as configurações tradicionais de um ou vários data centers. Ao distribuir recursos em várias zonas de disponibilidade em uma região, as aplicações e os bancos de dados podem ser projetados para realizar o failover automático entre as zonas sem qualquer interrupção no serviço. Esse nível de redundância e alta disponibilidade é um requisito essencial para workloads de missão crítica e permite que as organizações criem soluções resilientes nativas da nuvem.

Além disso, a escala e o alcance global da infraestrutura da AWS permitem que os clientes implantem suas aplicações mais perto dos usuários finais, reduzindo a latência e melhorando

a experiência geral do usuário. A disponibilidade de várias regiões em todo o mundo também possibilita a soberania e a conformidade efetivas dos dados, pois os clientes podem armazenar e processar dados dentro dos limites geográficos exigidos por suas necessidades regulatórias e comerciais específicas.

Ao aproveitar a infraestrutura global da AWS, as organizações podem arquitetar seus ambientes de nuvem para que sejam altamente disponíveis, tolerantes a falhas e escaláveis, munidos de flexibilidade para se adaptar às mudanças nos requisitos e às necessidades comerciais em evolução. Essa base robusta é um facilitador essencial para a implementação bem-sucedida de aplicações e serviços modernos baseados na nuvem.

Para obter mais informações sobre Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura global AWS.

É possível configurar suas VPCs para atender aos requisitos de resiliência das suas workloads. Para obter mais informações, consulte:

- Entenda os padrões de resiliência e as compensações (Blog de arquitetura da AWS)
- Planeje sua topologia de rede (AWS Well-Architected Framework)
- Opções de conectividade da Amazon Virtual Private Cloud (whitepapers da AWS)

Validação de conformidade da Amazon Virtual Private Cloud

Para saber se um AWS service (Serviço da AWS) está no escopo de programas de conformidade específicos, consulte Serviços da AWS no escopo por programa de conformidade e selecione o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de Conformidade da AWS.

É possível baixar relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Baixar relatórios no AWS Artifact.

Sua responsabilidade de conformidade ao usar o Serviços da AWS é determinada pela confidencialidade dos seus dados, pelos objetivos de conformidade da sua empresa e pelos regulamentos e leis aplicáveis. A AWS fornece os recursos a seguir para ajudar com a conformidade:

- Governança e conformidade de segurança: esses guias de implementação de solução abordam considerações sobre a arquitetura e fornecem etapas para implantar recursos de segurança e conformidade.

- Referência de serviços qualificados para HIPAA: lista os serviços qualificados para HIPAA. Nem todos os Serviços da AWS estão qualificados pela HIPAA.
- Recursos de Conformidade da AWS: essa coleção de manuais e guias pode ser aplicada ao seu setor e local.
- Guias de conformidade do cliente da AWS: entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as práticas recomendadas para proteção de Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliar recursos com regras no Guia do desenvolvedor do AWS Config: o serviço AWS Config avalia como as configurações de recursos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- AWS Security Hub: este AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança na AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty: este AWS service (Serviço da AWS) detecta possíveis ameaças às suas Contas da AWS, workloads, contêineres e dados ao monitorar o ambiente em busca de atividades suspeitas e maliciosas. O GuardDuty pode ajudar você a atender a diversos requisitos de conformidade, como o PCI DSS, com o cumprimento dos requisitos de detecção de intrusões requeridos por determinadas estruturas de conformidade.
- AWS Audit Manager: este AWS service (Serviço da AWS) ajuda você a auditar continuamente o seu uso da AWS para simplificar o modo como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

Bloquear o acesso público a VPCs e sub-redes

Bloquear o Acesso Público (BPA) da VCP é um atributo de segurança centralizado que confere a você autoridade para impedir o acesso público pela Internet aos recursos da VPC em toda a conta da AWS, garantindo conformidade com os requisitos de segurança e flexibilidade para permitir determinadas exceções e recursos de auditoria.

O atributo BPA da VPC tem os seguintes modos:

- Bidirecional: todo o tráfego de e para gateways da Internet e gateways da Internet somente de saída nesta região (exceto VPCs e sub-redes excluídas) é bloqueado.
- Somente de entrada: todo o tráfego de Internet para as VPCs dessa região (exceto as VPCs ou sub-redes excluídas) é bloqueado. Apenas o tráfego de e para gateways NAT e gateways da Internet somente de saída é permitido porque esses gateways só permitem o estabelecimento de conexões de saída.

É possível também pode criar "exclusões" desse atributo para tráfego que você não queira bloquear. Uma exclusão é um modo que pode ser aplicado a uma única VPC ou sub-rede que a isenta do modo de BPA da conta e permitirá acesso bidirecional ou somente de saída.

As exclusões podem ter um dos seguintes modos:

- Bidirecional: todo o tráfego de Internet para ou das VPCs e sub-redes excluídas é permitido.
- Somente de saída: o tráfego de Internet de saída das VPCs e sub-redes excluídas é permitido. O tráfego de Internet de entrada para as VPCs e sub-redes excluídas é bloqueado. Isso só se aplica quando o BPA está definido como bidirecional.

Conteúdo

Conceitos básicos do BPA

Esta seção aborda detalhes importantes sobre o BPA da VPC, incluindo quais são os serviços compatíveis e como você pode trabalhar com ele.

Conteúdo

- Criar e excluir exclusões
- Habilite o BPA da VPC no nível da organização

Disponibilidade regional

O BPA da VPC está disponível em todas as regiões comerciais da AWS, inclusive GovCloud e China.

Neste guia, você também encontrará informações sobre como usar o Analisador de Acesso à Rede e o Analisador de Acessibilidade com o BPA da VPC. Observe que o Analisador de Acesso à Rede e o Analisador de Acessibilidade não estão disponíveis em todas as regiões comerciais. Para obter informações sobre a disponibilidade regional do Analisador de Acesso à Rede e do Analisador de Acessibilidade, consulte Limitations no Network Access Analyzer Guide e Considerations no Reachability Analyzer Guide.

Impacto e compatibilidade dos serviços da AWS

Os seguintes recursos e serviços são compatíveis com o BPA da VPC e o tráfego para esses serviços e recursos é afetado pelo BPA da VPC:

- Gateway da Internet: todo o tráfego de entrada e saída é bloqueado.
- Gateway da Internet somente de saída: todo o tráfego de saída é bloqueado. Os gateways da Internet somente de saída não permitem tráfego de entrada.
- Gateway NAT: todo o tráfego de entrada e saída é bloqueado. Os gateways NAT exigem um gateway da Internet para conectividade com a Internet.
- Network Load Balancer voltado para a Internet: todo o tráfego de entrada e saída é bloqueado. Os Network Load Balancers de rede voltados para a Internet exigem um gateway da Internet para conectividade com a Internet.
- Application Load Balancer voltado para a Internet: todo o tráfego de entrada e saída é bloqueado. Os Application Load Balancers voltados para a Internet exigem um gateway da Internet para conectividade com a Internet.
- Amazon CloudFront VPC Origins: o tráfego de entrada e de saída é totalmente bloqueado.
- AWS Global Accelerator: o tráfego de entrada para as VPCs é bloqueado, independentemente de o destino estar ou não acessível pela Internet.
- Gateways da operadora do AWS Wavelength: o tráfego de entrada e de saída é totalmente bloqueado.

Tráfego relacionado com conectividade privada, como o tráfego dos seguintes serviços e recursos, não é bloqueado nem afetado pelo BPA da VPC:

- AWS Client VPN
- AWS CloudWAN
- Gateway local do AWS Outposts
- AWS Site-to-Site VPN
- Transit gateway
- Acesso Verificado pela AWS

> **Important**
>
> O tráfego enviado de forma privada e proveniente dos recursos na sua VPC para outros serviços em execução na mesma VPC, como o resolvedor de DNS do EC2 ou o Amazon OpenSearch Service, é permitido mesmo quando o BPA está ativado, pois não passa por um gateway da Internet na sua VPC. É possível que esses serviços façam solicitações a recursos fora da VPC em seu nome, por exemplo, para resolver uma consulta ao DNS, e podem expor informações sobre as atividades dos recursos da VPC, se isso não for mitigado por outros controles de segurança.

Limitações do BPA

O modo somente de entrada do BPA da VPC não é compatível com zonas locais (LZs) onde gateways NAT e gateways da Internet somente de saída não são permitidos.

Controle do acesso ao BPA da VPC com uma política do IAM

Para obter exemplos de políticas do IAM que permitem/negam acesso ao atributo BPA da VPC, consulte Bloquear o acesso público a VPCs e sub-redes.

Habilitar o modo bidirecional do BPA na sua conta

O modo bidirecional do BPA da VPC bloqueia todo o tráfego de e para os gateways da Internet e os gateways da Internet somente de saída nessa região (exceto em VPCs e sub-redes excluídas). Para obter mais informações sobre exclusões, consulte Criar e excluir exclusões.

> **Important**
>
> É extremamente recomendável analisar cuidadosamente as workloads que exigem acesso à Internet antes de habilitar o BPA da VPC em contas de produção.

> **Note**
>
> - Para habilitar o BPA da VPC nas VPCs e sub-redes da sua conta, você deve ser o proprietário das VPCs e das sub-redes.
> - Se você estiver compartilhando sub-redes da VPC com outras contas, o modo do BPA da VPC imposto pelo proprietário da sub-rede também se aplicará ao tráfego de participantes, mas os participantes não poderão controlar as configurações do BPA da VPC que afetam a sub-rede compartilhada.

AWS Management Console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação esquerdo, escolha Configurações.
3. Escolha Editar configurações de acesso público.
4. Escolha Ativar bloquear acesso público e Bidirecional e depois escolha Salvar alterações.
5. Aguarde até que Status mude para Ativado. Pode demorar alguns minutos para as configurações do BPA terem efeito e o status ser atualizado.

O modo bidirecional do BPA da VPC agora está ativado.

AWS CLI

1. Ativar o BPA da VPC:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-gateway-block-mode block-bidirectional
```

Pode demorar alguns minutos para as configurações do BPA terem efeito e o status ser atualizado.

2. Visualize o status do BPA da VPC:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

Alterar o modo do BPA da VPC para somente de entrada

O modo somente de entrada do BPA da VPC bloqueia todo o tráfego de Internet para as VPCs dessa região (exceto para VPCs ou sub-redes excluídas). Apenas o tráfego de e para gateways NAT e gateways da Internet somente de saída é permitido porque esses gateways só permitem o estabelecimento de conexões de saída.

AWS Management Console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação esquerdo, escolha Configurações.
3. Escolha Editar configurações de acesso público.
4. Altere a direção como Somente entrada.
5. Salve as alterações e aguarde a atualização do status. Pode demorar alguns minutos para as configurações do BPA terem efeito e o status ser atualizado.

AWS CLI

1. Modifique a direção do bloqueio do BPA da VPC:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-
gateway-block-mode block-ingress
```

   Pode demorar alguns minutos para as configurações do BPA terem efeito e o status ser atualizado.

2. Visualize o status do BPA da VPC:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

Criar e excluir exclusões

A exclusão do BPA da VPC é um modo que pode ser aplicado a uma única VPC ou sub-rede que a isenta do modo BPA da conta e permite acesso bidirecional ou somente de saída. Você pode criar exclusões do BPA para VPCs e sub-redes mesmo quando o BPA não está habilitado na conta para garantir que não haja interrupção do tráfego para as exclusões quando o BPA da VPC estiver ativado. Se uma VPC for excluída, essa exclusão será automaticamente aplicada a todas as suas sub-redes.

Você pode criar até 50 exclusões. Para obter informações sobre solicitação de aumento de limite, consulte VPC BPA exclusions per account em Cotas da Amazon VPC.

AWS Management Console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação esquerdo, escolha Configurações.
3. Acesse a guia Bloquear acesso público e, em Exclusões, realize uma das seguintes ações:
   - Para excluir uma exclusão, selecione-a e, em seguida, escolha Ações > Excluir exclusões.
   - Para criar uma exclusão, selecione Criar exclusões e prossiga com as próximas etapas.
4. Escolha uma direção para o bloqueio:
   - Bidirecional: permite todo o tráfego de Internet de e para as VPCs e sub-redes excluídas.
   - Somente de saída: permite o tráfego de Internet de saída das VPC e sub-redes excluídas. Bloqueia o tráfego de Internet de entrada para as VPCs e sub-redes excluídas. Essa configuração se aplica quando o BPA é definido como Bidirecional.
5. Escolha uma VPC ou uma sub-rede.
6. Escolha Criar exclusões.
7. Aguarde até que o status de Exclusão mude para Ativo. Pode ser necessário atualizar a tabela de exclusão para ver a alteração.

A exclusão foi criada.

AWS CLI

1. Modifique a direção de permissão da exclusão:

```
aws ec2 --region us-east-2 create-vpc-block-public-access-exclusion --subnet-
id subnet-id --internet-gateway-exclusion-mode allow-bidirectional
```

2. Pode levar algum tempo para o status da exclusão ser atualizado. Para visualizar o status da exclusão:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusions --
exclusion-ids exclusion-id
```

Habilite o BPA da VPC no nível da organização

Se você estiver usando o AWS Organizations para gerenciar contas na sua organização, poderá usar uma política declarativa do AWS Organizations para aplicar o BPA da VPC nas contas da organização. Para obter mais informações sobre a política declarativa do BPA da VPC, consulte Supported declarative policies no Guia do usuário do AWS Organizations.

> **Note**
>
> - É possível usar a política declarativa do BPA da VPC para configurar se as exclusões são permitidas, mas não é possível criar exclusões com a política. Para criar exclusões, é necessário fazê-lo na conta proprietária da VPC. Para obter mais informações sobre como criar exclusões do BPA da VPC, consulte Criar e excluir exclusões.
> - Caso a política declarativa do BPA da VPC esteja habilitada, nas configurações de bloqueio de acesso público, será exibido Gerenciado por política declarativa e você não poderá modificar as configurações do BPA da VPC no nível da conta.

Avaliar o impacto e monitorar o BPA

Esta seção contém informações sobre como avaliar o impacto do BPA da VPC antes de ativá-lo e como monitorar se o tráfego está sendo bloqueado depois de ativá-lo.

Conteúdo

- Verificar se a conectividade é bloqueada com o Analisador de Acessibilidade

Avaliar o impacto do BPA com o Access Analyzer de rede

Nesta seção, você usará o Access Analyzer de rede para visualizar os recursos da sua conta que usam um gateway da Internet antes de habilitar o BPA da VPC e bloquear o acesso. Use essa análise para entender o impacto de ativar o BPA da VPC em sua conta e de bloquear o tráfego.

> **Note**
>
> - O Analisador de Acesso à Rede não é compatível com IPv6; portanto, você não poderá usá-lo para visualizar o impacto potencial do BPA no tráfego IPv6 de saída do gateway da Internet somente de saída.
> - As análises realizadas com o Analisador de Acesso à Rede são cobradas. Para obter mais informações, consulte Pricing no Access Analyzer de rede Guide.
> - Para obter informações sobre a disponibilidade regional do Analisador de Acesso à Rede, consulte Limitations no Network Access Analyzer Guide.

AWS Management Console

1. Abra o console do AWS Network Insights em https://console.aws.amazon.com/networkinsights/.
2. Escolha Analisador de Acesso à Rede.
3. Escolha Criar escopo de acesso à rede.
4. Escolha Avaliar o impacto do Bloqueio de Acesso Público da VPC e clique em Próximo.
5. O modelo já está configurado para analisar o tráfego de e para os gateways da Internet da sua conta. Você pode visualizar isso em Origem e Destino.
6. Escolha Próximo.
7. Escolha Criar escopo de acesso à rede.
8. Escolha o escopo que você acabou de criar e escolha Analisar.
9. Aguarde a conclusão da análise.
10. Visualizar as descobertas da análise. Cada linha em Descobertas mostra um caminho de rede que um pacote pode percorrer em uma rede de ou para um gateway da Internet na sua

conta. Nesse caso, se você ativar o BPA da VPC e nenhuma das VPCs e/ou sub-redes que aparecerem nessas descobertas estiverem configuradas como exclusões do BPA, o tráfego para essas VPCs e sub-redes será restringido.

11. Analise cada descoberta para entender o impacto do BPA nos recursos das VPCs.

A análise de impacto foi concluída.

AWS CLI

1. Crie um escopo de acesso à rede:

```
aws ec2 create-network-insights-access-scope --region us-east-2 --match-paths
 "Source={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
 "Destination={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
```

2. Inicie a análise do escopo:

```
aws ec2 start-network-insights-access-scope-analysis  --region us-east-2 --
network-insights-access-scope-id nis-id
```

3. Obtenha os resultados da análise:

```
aws ec2 get-network-insights-access-scope-analysis-findings  --region us-east-2
 --network-insights-access-scope-analysis-id nisa-0aa383a1938f94cd1 --max-items
 1
```

Os resultados mostram o tráfego de e para os gateways da Internet em todas as VPCs da sua conta. Os resultados são organizados como "descobertas". "FindingId": "AnalysisFinding-1" indica que essa é a primeira descoberta da análise. Observe que há várias descobertas e cada uma indica um fluxo de tráfego que será afetado pela ativação do BPA da VPC. A primeira descoberta mostrará que o tráfego começou em um gateway da Internet ("SequenceNumber": 1), passou para uma NACL ("SequenceNumber": 2), para um grupo de segurança ("SequenceNumber": 3) e terminou em uma instância ("SequenceNumber": 4).

4. Analise as descobertas para entender o impacto do BPA nos recursos das VPCs.

A análise de impacto foi concluída.

Monitorar o impacto do BPA com logs de fluxo

Os logs de fluxo da VPC são um atributo que permite capturar informações sobre o tráfego de e para as interfaces de rede elásticas da VPC. Você pode usar esse atributo para monitorar o tráfego que é impedido pelo BPA da VPC de chegar às interfaces de rede da sua instância.

Crie um log de fluxo para a VPC usando as etapas em Trabalhar com logs de fluxo.

Quando você criar o log de fluxo, certifique-se de usar um formato personalizado que inclua o campo `reject-reason`.

Quando visualizar os logs de fluxo, se o tráfego para uma ENI for rejeitado devido ao BPA, você verá um `reject-reason` de `BPA` na entrada do log de fluxo.

Além das limitações padrão dos logs de fluxo da VPC, observe as seguintes limitações específicas do BPA da VPC:

- Os logs de fluxo para o BPA da VPC não incluem os registros ignorados.
- Os logs de fluxo para o BPA da VPC não incluem `bytes` mesmo que você inclua o campo `bytes` no log de fluxo.

Rastrear a remoção de exclusões com o CloudTrail

Esta seção explica como você pode usar o AWS CloudTrail para monitorar e rastrear a remoção de exclusões do BPA da VPC.

AWS Management Console

Você pode visualizar todas as exclusões removidas no histórico de eventos do CloudTrail consultando Tipo de recurso > `AWS::EC2::VPCBlockPublicAccessExclusion` > no console do AWS CloudTrail em https://console.aws.amazon.com/cloudtrailv2/.

AWS CLI

Você pode usar o comando `lookup-events` para visualizar os eventos relacionados com remoção de exclusões:

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceType,AttributeValue=AWS::EC2::VPCBlockPublicAccessExclusion
```

Verificar se a conectividade é bloqueada com o Analisador de Acessibilidade

O Analisador de Acessibilidade da VPC pode ser usado para avaliar se determinados caminhos de rede podem ou não ser acessados de acordo com sua configuração de rede, incluindo as configurações do BPA da VPC.

Para obter informações sobre a disponibilidade regional do Analisador de Acessibilidade, consulte Considerations no Reachability Analyzer Guide.

AWS Management Console

1. Abra o console do AWS Network Insights em https://console.aws.amazon.com/networkinsights/home#ReachabilityAnalyzer.
2. Clique em Criar e analisar caminho.
3. Em Tipo de origem, escolha Gateways da Internet e selecione o gateway da Internet do qual você deseja bloquear tráfego na lista suspensa Origem.
4. Em Tipo de destino, escolha Instâncias e selecione a instância para a qual você deseja bloquear tráfego no menu suspenso Destino.
5. Clique em Criar e analisar caminho.
6. Aguarde a conclusão da análise. Pode levar alguns minutos.
7. Após a conclusão, você verá que o Status de acessibilidade é Não acessível e que Detalhes do caminho mostra que `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` é a causa desse problema de acessibilidade.

AWS CLI

1. Crie um caminho de rede usando o ID do gateway da Internet do qual você deseja bloquear tráfego (origem) e o ID da instância para a qual você deseja bloquear tráfego (destino):

```
aws ec2 --region us-east-2 create-network-insights-path --source igw-id --
destination instance-id --protocol TCP
```

2. Inicie uma análise no caminho da rede:

```
aws ec2 --region us-east-2 start-network-insights-analysis --network-insights-
path-id nip-id
```

3. Recupere os resultados da análise:

```
aws ec2 --region us-east-2 describe-network-insights-analyses --network-
insights-analysis-ids nia-id
```

4. Verifique se `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` é o `ExplanationCode` para a falta de acessibilidade.

Exemplo avançado

Esta seção contém um exemplo avançado que ajudará a entender como o atributo Bloquear o Acesso Público da VPC funciona em diferentes cenários. Todo cenário se baseia no cenário anterior, por isso é importante concluir as etapas em ordem.

> **Important**
>
> Não teste esse exemplo em uma conta de produção. É extremamente recomendável analisar cuidadosamente as workloads que exigem acesso à Internet antes de habilitar o BPA da VPC em contas de produção.

> **Note**
>
> Para entender completamente o atributo BPA da VPC, você precisará de alguns recursos da sua conta. Nesta seção, fornecemos um modelo do AWS CloudFormation que você pode usar para provisionar os recursos necessários para entender totalmente como esse atributo funciona. Há custos associados aos recursos que você provisiona com o modelo CloudFormation e às análises que realiza com o Analisador de Acesso à Rede e o Analisador de Acessibilidade. Se você usar o modelo desta seção, certifique-se de concluir as etapas de limpeza quando terminar com o exemplo.

Conteúdo

- Cenário 4: criar uma exclusão
- Cenário 5: modificar o modo de exclusão
- Cenário 6: modificar o modo do BPA
- Limpeza

Implantar modelo do CloudFormation

Para demonstrar como esse atributo funciona, você precisa de uma VPC, sub-redes, instâncias e outros recursos. Para facilitar a realização desta demonstração, fornecemos abaixo um modelo do AWS CloudFormation que você pode usar para iniciar rapidamente os recursos necessários para os cenários desta demonstração.

> **Note**
>
> Há custos associados aos recursos que você cria nesta seção com o modelo do CloudFormation, como o custo do gateway NAT e dos endereços IPv4 públicos. Para evitar custos excessivos, não deixe de realizar as etapas de limpeza para remover todos os recursos criados para este exemplo.

O modelo cria os seguintes recursos na sua conta:

- Gateway da Internet somente de saída
- Gateway da Internet
- nat gateway
- Duas sub-redes públicas
- Uma sub-rede privada
- Duas instâncias do EC2 com endereços IPv4 privados e públicos
- Uma instância do EC2 com um endereço IPv6 e um endereço IPv4 privado
- Uma instância do EC2 apenas com um endereço IPv4 privado
- Grupo de segurança com tráfego de entrada SSH e ICMP permitido e TODO o tráfego de saída permitido
- Log do fluxo da VPC
- Um endpoint do EC2 Instance Connect na sub-rede B

Copie o modelo abaixo e salve-o em um arquivo .yaml.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Creates a VPC with public and private subnets, NAT gateway, and EC2
 instances for VPC BPA.

Parameters:
  InstanceAMI:
    Description: ID of the Amazone Machine Image (AMI) to use with the instances
 launched by this template
    Type: AWS::EC2::Image::Id
  InstanceType:
    Description: EC2 Instance type to use with the instances launched by this template
    Type: String
    Default: t2.micro

Resources:

  # VPC
  VPCBPA:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.0.0.0/16
      EnableDnsHostnames: true
      EnableDnsSupport: true
      InstanceTenancy: default
      Tags:
        - Key: Name
          Value: VPC BPA

  # VPC IPv6 CIDR
  VPCBPAIpv6CidrBlock:
    Type: AWS::EC2::VPCCidrBlock
    Properties:
      VpcId: !Ref VPCBPA
      AmazonProvidedIpv6CidrBlock: true

  # EC2 Key Pair
  VPCBPAKeyPair:
    Type: AWS::EC2::KeyPair
    Properties:
      KeyName: vpc-bpa-key

  # Internet Gateway
```

```
  VPCBPAInternetGateway:
    Type: AWS::EC2::InternetGateway
    Properties:
      Tags:
        - Key: Name
          Value: VPC BPA Internet Gateway

  VPCBPAInternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      VpcId: !Ref VPCBPA
      InternetGatewayId: !Ref VPCBPAInternetGateway

  # Egress-Only Internet Gateway
  VPCBPAEgressOnlyInternetGateway:
    Type: AWS::EC2::EgressOnlyInternetGateway
    Properties:
      VpcId: !Ref VPCBPA

  # Subnets
  VPCBPAPublicSubnetA:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPCBPA
      CidrBlock: 10.0.1.0/24
      MapPublicIpOnLaunch: true
      Tags:
        - Key: Name
          Value: VPC BPA Public Subnet A

  VPCBPAPublicSubnetB:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPCBPA
      CidrBlock: 10.0.2.0/24
      MapPublicIpOnLaunch: true
      Tags:
        - Key: Name
          Value: VPC BPA Public Subnet B

  VPCBPAPrivateSubnetC:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPCBPA
```

```
      CidrBlock: 10.0.3.0/24
      MapPublicIpOnLaunch: false
      Ipv6CidrBlock: !Select [0, !GetAtt VPCBPA.Ipv6CidrBlocks]
      AssignIpv6AddressOnCreation: true
      Tags:
        - Key: Name
          Value: VPC BPA Private Subnet C

  # NAT Gateway
  VPCBPANATGateway:
    Type: AWS::EC2::NatGateway
    Properties:
      AllocationId: !GetAtt VPCBPANATGatewayEIP.AllocationId
      SubnetId: !Ref VPCBPAPublicSubnetB
      Tags:
        - Key: Name
          Value: VPC BPA NAT Gateway

  VPCBPANATGatewayEIP:
    Type: AWS::EC2::EIP
    Properties:
      Domain: vpc
      Tags:
        - Key: Name
          Value: VPC BPA NAT Gateway EIP

  # Route Tables
  VPCBPAPublicRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref VPCBPA
      Tags:
        - Key: Name
          Value: VPC BPA Public Route Table

  VPCBPAPublicRoute:
    Type: AWS::EC2::Route
    DependsOn: VPCBPAInternetGatewayAttachment
    Properties:
      RouteTableId: !Ref VPCBPAPublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref VPCBPAInternetGateway

  VPCBPAPublicSubnetARouteTableAssoc:
```

```
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      SubnetId: !Ref VPCBPAPublicSubnetA
      RouteTableId: !Ref VPCBPAPublicRouteTable

  VPCBPAPublicSubnetBRouteTableAssoc:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      SubnetId: !Ref VPCBPAPublicSubnetB
      RouteTableId: !Ref VPCBPAPublicRouteTable

  VPCBPAPrivateRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref VPCBPA
      Tags:
        - Key: Name
          Value: VPC BPA Private Route Table

  VPCBPAPrivateRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref VPCBPAPrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref VPCBPANATGateway

  VPCBPAPrivateSubnetCRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref VPCBPAPrivateRouteTable
      DestinationIpv6CidrBlock: ::/0
      EgressOnlyInternetGatewayId: !Ref VPCBPAEgressOnlyInternetGateway

  VPCBPAPrivateSubnetCRouteTableAssociation:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      SubnetId: !Ref VPCBPAPrivateSubnetC
      RouteTableId: !Ref VPCBPAPrivateRouteTable

  # EC2 Instances Security Group
  VPCBPAInstancesSecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupName: VPC BPA Instances Security Group
```

```
      GroupDescription: Allow SSH and ICMP access
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 22
          ToPort: 22
          CidrIp: 0.0.0.0/0
        - IpProtocol: icmp
          FromPort: -1
          ToPort: -1
          CidrIp: 0.0.0.0/0
      VpcId: !Ref VPCBPA
      Tags:
        - Key: Name
          Value: VPC BPA Instances Security Group

  # EC2 Instances
  VPCBPAInstanceA:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: !Ref InstanceAMI
      InstanceType: t2.micro
      KeyName: !Ref VPCBPAKeyPair
      SubnetId: !Ref VPCBPAPublicSubnetA
      SecurityGroupIds:
        - !Ref VPCBPAInstancesSecurityGroup
      Tags:
        - Key: Name
          Value: VPC BPA Instance A

  VPCBPAInstanceB:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: !Ref InstanceAMI
      InstanceType: !Ref InstanceType
      KeyName: !Ref VPCBPAKeyPair
      SubnetId: !Ref VPCBPAPublicSubnetB
      SecurityGroupIds:
        - !Ref VPCBPAInstancesSecurityGroup
      Tags:
        - Key: Name
          Value: VPC BPA Instance B

  VPCBPAInstanceC:
    Type: AWS::EC2::Instance
```

```
    Properties:
      ImageId: !Ref InstanceAMI
      InstanceType: !Ref InstanceType
      KeyName: !Ref VPCBPAKeyPair
      SubnetId: !Ref VPCBPAPrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCBPAInstancesSecurityGroup
      Tags:
        - Key: Name
          Value: VPC BPA Instance C

  VPCBPAInstanceD:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: !Ref InstanceAMI
      InstanceType: !Ref InstanceType
      KeyName: !Ref VPCBPAKeyPair
      NetworkInterfaces:
        - DeviceIndex: '0'
          GroupSet:
            - !Ref VPCBPAInstancesSecurityGroup
          SubnetId: !Ref VPCBPAPrivateSubnetC
          Ipv6AddressCount: 1
      Tags:
        - Key: Name
          Value: VPC BPA Instance D

  # Flow Logs IAM Role
  VPCBPAFlowLogRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service: vpc-flow-logs.amazonaws.com
            Action: 'sts:AssumeRole'
      Tags:
        - Key: Name
          Value: VPC BPA Flow Logs Role

  VPCBPAFlowLogPolicy:
    Type: AWS::IAM::Policy
```

```
    Properties:
      PolicyName: VPC-BPA-FlowLogsPolicy
      PolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Action:
              - 'logs:CreateLogGroup'
              - 'logs:CreateLogStream'
              - 'logs:PutLogEvents'
              - 'logs:DescribeLogGroups'
              - 'logs:DescribeLogStreams'
            Resource: '*'
      Roles:
        - !Ref VPCBPAFlowLogRole

  # Flow Logs
  VPCBPAFlowLog:
    Type: AWS::EC2::FlowLog
    Properties:
      ResourceId: !Ref VPCBPA
      ResourceType: VPC
      TrafficType: ALL
      LogDestinationType: cloud-watch-logs
      LogGroupName: /aws/vpc-flow-logs/VPC-BPA
      DeliverLogsPermissionArn: !GetAtt VPCBPAFlowLogRole.Arn
      LogFormat: '${version} ${account-id} ${interface-id} ${srcaddr} ${dstaddr}
 ${srcport} ${dstport} ${protocol} ${packets} ${bytes} ${start} ${end} ${action} ${log-
status} ${vpc-id} ${subnet-id} ${instance-id} ${tcp-flags} ${type} ${pkt-srcaddr}
 ${pkt-dstaddr} ${region} ${az-id} ${sublocation-type} ${sublocation-id} ${pkt-src-aws-
service} ${pkt-dst-aws-service} ${flow-direction} ${traffic-path} ${reject-reason}'
      Tags:
        - Key: Name
          Value: VPC BPA Flow Logs

  # EC2 Instance Connect Endpoint
  VPCBPAEC2InstanceConnectEndpoint:
    Type: AWS::EC2::InstanceConnectEndpoint
    Properties:
      SecurityGroupIds:
        - !Ref VPCBPAInstancesSecurityGroup
      SubnetId: !Ref VPCBPAPublicSubnetB

Outputs:
```

```
  VPCBPAVPCId:
    Description: A reference to the created VPC
    Value: !Ref VPCBPA
    Export:
      Name: vpc-id

  VPCBPAPublicSubnetAId:
    Description: The ID of the public subnet A
    Value: !Ref VPCBPAPublicSubnetA

  VPCBPAPublicSubnetAName:
    Description: The name of the public subnet A
    Value: VPC BPA Public Subnet A

  VPCBPAPublicSubnetBId:
    Description: The ID of the public subnet B
    Value: !Ref VPCBPAPublicSubnetB

  VPCBPAPublicSubnetBName:
    Description: The name of the public subnet B
    Value: VPC BPA Public Subnet B

  VPCBPAPrivateSubnetCId:
    Description: The ID of the private subnet C
    Value: !Ref VPCBPAPrivateSubnetC

  VPCBPAPrivateSubnetCName:
    Description: The name of the private subnet C
    Value: VPC BPA Private Subnet C

  VPCBPAInstanceAId:
    Description: The ID of instance A
    Value: !Ref VPCBPAInstanceA

  VPCBPAInstanceBId:
    Description: The ID of instance B
    Value: !Ref VPCBPAInstanceB

  VPCBPAInstanceCId:
    Description: The ID of instance C
    Value: !Ref VPCBPAInstanceC

  VPCBPAInstanceDId:
    Description: The ID of instance D
```

```
    Value: !Ref VPCBPAInstanceD
```

AWS Management Console

1. Abra o console do AWS CloudFormation em https://console.aws.amazon.com/cloudformation/.
2. Escolha Criar pilha e carregue o arquivo do modelo .yaml.
3. Siga as etapas para iniciar o modelo. Você precisará inserir um ID de imagem e um tipo de instância (como t2.micro). Será necessário também permitir que o CloudFormation crie para você um perfil do IAM para a criação do log de fluxo e permissão para fazer login no Amazon CloudWatch.
4. Depois de iniciar a pilha, na guia Eventos, visualize o andamento e certifique-se de que pilha esteja concluída antes de continuar.

AWS CLI

1. Execute o seguinte comando para criar a pilha do CloudFormation:

```
aws cloudformation create-stack --stack-name VPC-BPA-stack --template-body
 file://sampletemplate.yaml --capabilities CAPABILITY_IAM --region us-east-2
```

Saída:

```
{
    "StackId": "arn:aws:cloudformation:us-east-2:470889052923:stack/VPC-BPA-
stack/8a7a2cc0-8001-11ef-b196-06386a84b72f"
}
```

2. Visualize o andamento e certifique-se de que pilha esteja concluída antes de continuar:

```
aws cloudformation describe-stack-events --stack-name VPC-BPA-stack --region us-
east-2
```

Visualizar o impacto do BPA da VPC com o Analisador de Acesso à Rede

Nesta seção, você usará o Analisador de Acesso à Rede para visualizar os recursos da sua conta que usam um gateway da Internet. Use essa análise para entender o impacto de ativar o BPA da VPC em sua conta e de bloquear o tráfego.

Para obter informações sobre a disponibilidade regional do Analisador de Acesso à Rede, consulte Limitations no Network Access Analyzer Guide.

AWS Management Console

1. Abra o console do AWS Network Insights em https://console.aws.amazon.com/networkinsights/.
2. Escolha Analisador de Acesso à Rede.
3. Escolha Criar escopo de acesso à rede.
4. Escolha Avaliar o impacto do Bloqueio de Acesso Público da VPC e clique em Próximo.
5. O modelo já está configurado para analisar o tráfego de e para os gateways da Internet da sua conta. Você pode visualizar isso em Origem e Destino.
6. Escolha Próximo.
7. Escolha Criar escopo de acesso à rede.
8. Escolha o escopo que você acabou de criar e escolha Analisar.
9. Aguarde a conclusão da análise.
10. Visualizar as descobertas da análise. Cada linha em Descobertas mostra um caminho de rede que um pacote pode percorrer em uma rede de ou para um gateway da Internet na sua conta. Nesse caso, se você ativar o BPA da VPC e nenhuma das VPCs e/ou sub-redes que aparecerem nessas descobertas estiverem configuradas como exclusões do BPA, o tráfego para essas VPCs e sub-redes será restringido.
11. Analise cada descoberta para entender o impacto do BPA nos recursos das VPCs.

A análise de impacto foi concluída.

AWS CLI

1. Crie um escopo de acesso à rede:

```
aws ec2 create-network-insights-access-scope --match-paths
 "Source={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
```

```
 "Destination={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
 --region us-east-2
```

Saída:

```
{
  "NetworkInsightsAccessScope": {
    "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
    "NetworkInsightsAccessScopeArn": "arn:aws:ec2:us-
east-2:470889052923:network-insights-access-scope/nis-04cad3c4b3a1d5e3e",
    "CreatedDate": "2024-09-30T15:55:53.171000+00:00",
    "UpdatedDate": "2024-09-30T15:55:53.171000+00:00"
  },
  "NetworkInsightsAccessScopeContent": {
    "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
    "MatchPaths": [
      {
        "Source": {
          "ResourceStatement": {
            "ResourceTypes": [
              "AWS::EC2::InternetGateway"
            ]
          }
        }
      },
      {
        "Destination": {
          "ResourceStatement": {
            "ResourceTypes": [
              "AWS::EC2::InternetGateway"
            ]
          }
        }
      }
    ]
  }
}
```

2. Inicie a análise do escopo:

```
aws ec2 start-network-insights-access-scope-analysis --network-insights-access-
scope-id nis-04cad3c4b3a1d5e3e --region us-east-2
```

Saída:

```
{
  "NetworkInsightsAccessScopeAnalysis": {
    "NetworkInsightsAccessScopeAnalysisId": "nisa-0aa383a1938f94cd1",
    "NetworkInsightsAccessScopeAnalysisArn": "arn:aws:ec2:us-
east-2:470889052923:network-insights-access-scope-analysis/
nisa-0aa383a1938f94cd",
    "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
    "Status": "running",
    "StartDate": "2024-09-30T15:56:59.109000+00:00",
    "AnalyzedEniCount": 0
  }
}
```

3. Obtenha os resultados da análise:

```
aws ec2 get-network-insights-access-scope-analysis-findings --network-insights-
access-scope-analysis-id nisa-0aa383a1938f94cd1 --region us-east-2 --max-items 1
```

Saída:

```
{
  "AnalysisFindings": [
    {
      "NetworkInsightsAccessScopeAnalysisId": "nisa-0aa383a1938f94cd1",
      "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
      "FindingId": "AnalysisFinding-1",
      "FindingComponents": [
        {
          "SequenceNumber": 1,
          "Component": {
            "Id": "igw-04a5344b4e30486f1",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:internet-gateway/
igw-04a5344b4e30486f1",
            "Name": "VPC BPA Internet Gateway"
          },
          "OutboundHeader": {
            "DestinationAddresses": [
              "10.0.1.85/32"
            ]
          },
```

```
          "InboundHeader": {
            "DestinationAddresses": [
              "10.0.1.85/32"
            ],
            "DestinationPortRanges": [
              {
                "From": 22,
                "To": 22
              }
            ],
            "Protocol": "6",
            "SourceAddresses": [
              "0.0.0.0/5",
              "100.0.0.0/10",
              "96.0.0.0/6"
            ],
            "SourcePortRanges": [
              {
                "From": 0,
                "To": 65535
              }
            ]
          },
          "Vpc": {
            "Id": "vpc-0762547ec48b6888d",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:vpc/
vpc-0762547ec48b6888d",
            "Name": "VPC BPA"
          }
        },
        {
          "SequenceNumber": 2,
          "AclRule": {
            "Cidr": "0.0.0.0/0",
            "Egress": false,
            "Protocol": "all",
            "RuleAction": "allow",
            "RuleNumber": 100
          },
          "Component": {
            "Id": "acl-06194fc3a4a03040b",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:network-acl/
acl-06194fc3a4a03040b"
          }
```

```
        },
        {
          "SequenceNumber": 3,
          "Component": {
            "Id": "sg-093dde06415d03924",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:security-group/
sg-093dde06415d03924",
            "Name": "VPC BPA Instances Security Group"
          },
          "SecurityGroupRule": {
            "Cidr": "0.0.0.0/0",
            "Direction": "ingress",
            "PortRange": {
              "From": 22,
              "To": 22
            },
            "Protocol": "tcp"
          }
        },
        {
          "SequenceNumber": 4,
          "AttachedTo": {
            "Id": "i-058db34f9a0997895",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:instance/
i-058db34f9a0997895",
            "Name": "VPC BPA Instance A"
          },
          "Component": {
            "Id": "eni-0fa23f2766f03b286",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:network-interface/
eni-0fa23f2766f03b286"
          },
          "InboundHeader": {
            "DestinationAddresses": [
              "10.0.1.85/32"
            ],
            "DestinationPortRanges": [
              {
                "From": 22,
                "To": 22
              }
            ],
            "Protocol": "6",
            "SourceAddresses": [
```

```
              "0.0.0.0/5",
              "100.0.0.0/10",
              "96.0.0.0/6"
            ],
            "SourcePortRanges": [
              {
                "From": 0,
                "To": 65535
              }
            ]
          },
          "Subnet": {
            "Id": "subnet-035d235a762eeed04",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:subnet/
subnet-035d235a762eeed04",
            "Name": "VPC BPA Public Subnet A"
          },
          "Vpc": {
            "Id": "vpc-0762547ec48b6888d",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:vpc/
vpc-0762547ec48b6888d",
            "Name": "VPC BPA"
          }
        }
      ]
    }
  ],
  "AnalysisStatus": "succeeded",
  "NetworkInsightsAccessScopeAnalysisId": "nisa-0aa383a1938f94cd1",
  "NextToken":
 "eyJOZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfQ=="
}
```

Os resultados mostram o tráfego de e para os gateways da Internet em todas as VPCs da sua conta. Os resultados são organizados como "descobertas". "FindingId": "AnalysisFinding-1" indica que essa é a primeira descoberta da análise. Observe que há várias descobertas e cada uma indica um fluxo de tráfego que será afetado pela ativação do BPA da VPC. A primeira descoberta mostrará que o tráfego começou em um gateway da Internet ("SequenceNumber": 1), passou para uma NACL ("SequenceNumber": 2), para um grupo de segurança ("SequenceNumber": 3) e terminou em uma instância ("SequenceNumber": 4).

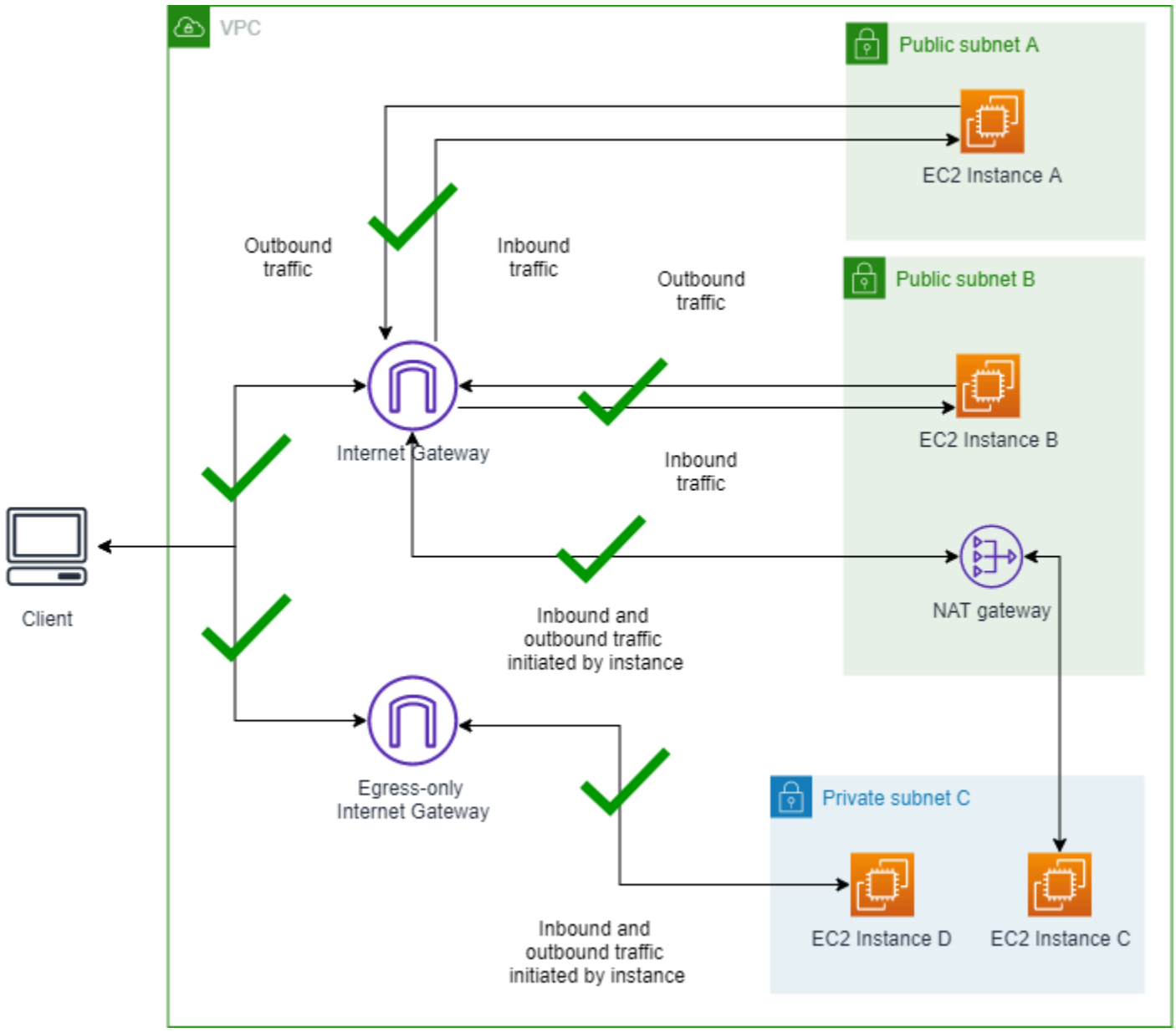
4. Analise as descobertas para entender o impacto do BPA nos recursos das VPCs.

A análise de impacto foi concluída.

Cenário 1: estabelecer conexão com instâncias quando o BPA não está ativado

Nesta seção, para definir uma linha de base e garantir, antes de habilitar o BPA, que todas as instâncias possam ser acessadas, você se conectará a todas as instâncias e emitirá um ping para um endereço IP público.

Diagrama de uma VPC sem o BPA da VPC ativado:



1.1 Conectar-se a instâncias

Conclua esta seção para se conectar às suas instâncias com o BPA da VPC desativado para garantir que você possa se conectar sem problemas. Todas as instâncias criadas com o CloudFormation neste exemplo têm nomes como "Instância A do BPA da VPC".

AWS Management Console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Abra os detalhes da instância A.
3. Para se conectar à instância A, use a opção EC2 Instance Connect > Estabelecer conexão usando o endpoint do EC2 Instance Connect.
4. Selecione Conectar. Depois de se conectar com sucesso à instância, emita um ping para www.amazon.com para verificar se você pode enviar solicitações de saída à Internet.
5. Use o mesmo método que você utilizou para estabelecer conexão com a instância A para acessar as instâncias B, C e D. De cada uma delas, execute um ping em www.amazon.com para confirmar se é possível enviar solicitações de saída para a Internet.

AWS CLI

1. Emita um ping para a instância A usando o endereço IPv4 público para verificar se há tráfego de entrada:

   ```
   ping 18.225.8.244
   ```

   Saída:

   ```
   Pinging 18.225.8.244 with 32 bytes of data:

   Reply from 18.225.8.244: bytes=32 time=51ms TTL=110
   Reply from 18.225.8.244: bytes=32 time=61ms TTL=110
   ```

   Observe que o ping foi bem-sucedido e o tráfego não está bloqueado.
2. Use o endereço IPv4 privado para se conectar e verificar se há tráfego de saída:

   ```
   aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
   east-2 --connection-type eice
   ```

Saída:

```
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
/ /
/m/'
Last login: Fri Sep 27 18:27:57 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING www-amazon-com.customer.fastly.net (18.65.233.187) 56(84) bytes of data.
64 bytes from 18.65.233.187 (18.65.233.187): icmp_seq=15 ttl=58 time=2.06 ms
64 bytes from 18.65.233.187 (18.65.233.187): icmp_seq=16 ttl=58 time=2.26 ms
```

Observe que o ping foi bem-sucedido e o tráfego não está bloqueado.

3. Emita um ping para a instância B usando o endereço IPv4 público para verificar se há tráfego de entrada:

```
ping 3.18.106.198
```

Saída:

```
Pinging 3.18.106.198 with 32 bytes of data:
Reply from 3.18.106.198: bytes=32 time=83ms TTL=110
Reply from 3.18.106.198: bytes=32 time=54ms TTL=110
```

Observe que o ping foi bem-sucedido e o tráfego não está bloqueado.

4. Use o endereço IPv4 privado para se conectar e verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id  i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

Saída:

```
A newer release of "Amazon Linux" is available.
Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
/ /
/m/'
Last login: Fri Sep 27 18:12:27 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=249 time=1.55 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=249 time=1.67 ms
```

Observe que o ping foi bem-sucedido e o tráfego não está bloqueado.

5. Conecte-se à instância C. Como não há endereço IP público para o qual emitir um ping, use o EC2 Instance Connect para se conectar e depois emita um ping da instância para um IP público para verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Saída:

```
A newer release of "Amazon Linux" is available.
Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
/ /
/m/'
```

```
Last login: Thu Sep 19 20:31:26 2024 from 10.0.2.86
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=248 time=1.75 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=248 time=1.97 ms
64 bytes from server-3-160-24-26.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=3 ttl=248 time=1.08 ms
```

Observe que o ping foi bem-sucedido e o tráfego não está bloqueado.

6. Conecte-se à instância D. Como não há endereço IP público para o qual emitir um ping, use o EC2 Instance Connect para se conectar e depois emita um ping da instância para um IP público para verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Saída:

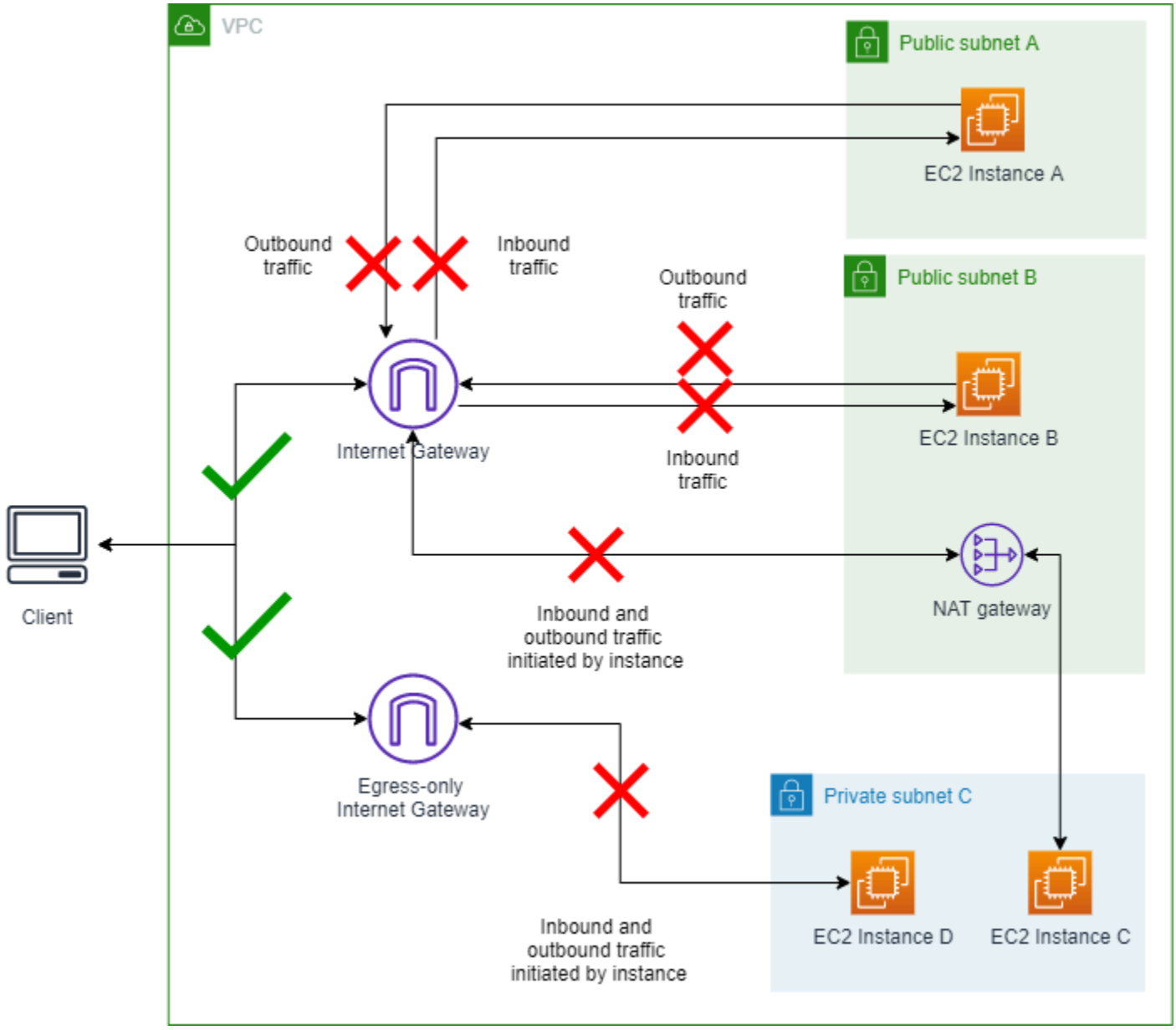
```
The authenticity of host '10.0.3.59 can't be established.
ECDSA key fingerprint is SHA256:c4naBCqbC61/cExDyccEproNU+1HHSpMSzl2J6cOtIZA8g.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.3.59' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ _/
_/m/'
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:ee00:7:49a5:5fd4:b121
 (2600:9000:25f3:ee00:7:49a5:5fd4:b121)) 56 data bytes
64 bytes from 2600:9000:25f3:ee00:7:49a5:5fd4:b121
 (2600:9000:25f3:ee00:7:49a5:5fd4:b121): icmp_seq=1 ttl=58 time=1.19 ms
64 bytes from 2600:9000:25f3:ee00:7:49a5:5fd4:b121
 (2600:9000:25f3:ee00:7:49a5:5fd4:b121): icmp_seq=2 ttl=58 time=1.38 ms
```

Observe que o ping foi bem-sucedido e o tráfego não está bloqueado.

Cenário 2: ativar o BPA

Nesta seção, você ativará o BPA da VPC e bloqueará o tráfego de e para os gateways da Internet em sua conta.

Diagrama do modo bidirecional do BPA da VPC ativado:



2.1 Habilitar o modo bidirecional de bloqueio do BPA da VPC

Conclua esta seção para habilitar o BPA da VPC.

AWS Management Console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação esquerdo, escolha Configurações.
3. Escolha Editar configurações de acesso público.
4. Escolha Ativar bloquear acesso público e Bidirecional e depois escolha Salvar alterações.
5. Aguarde até que Status mude para Ativado. Pode demorar alguns minutos para as configurações do BPA terem efeito e o status ser atualizado.

O BPA da VPC agora está ativado.

AWS CLI

1. Use o comando modify-vpc-block-public-access-options para ativar o BPA da VPC:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-gateway-block-mode block-bidirectional
```

Pode demorar alguns minutos para as configurações do BPA terem efeito e o status ser atualizado.

2. Visualize o status do BPA da VPC:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

2.2 Conectar-se a instâncias

Conclua esta seção para se conectar às suas instâncias.

AWS Management Console

1. Emita um ping para o endereço IPv4 público da instância A e da instância B, como fez no cenário 1. Observe que o tráfego está bloqueado.

2. Para se conectar à instância A, use a opção EC2 Instance Connect > Estabelecer conexão usando o endpoint do EC2 Instance Connect, como você fez no Cenário 1. Certifique-se de usar a opção de endpoint.
3. Selecione Conectar. Após se conectar com êxito à instância, execute um ping para www.amazon.com. Observe que todo o tráfego de saída está bloqueado.
4. Use o mesmo método que você utilizou para estabelecer conexão com a instância A para acessar as instâncias B, C e D para testar o envio de solicitações de saída para a Internet. Observe que todo o tráfego de saída está bloqueado.

AWS CLI

1. Emita um ping para a instância A usando o endereço IPv4 público para verificar se há tráfego de entrada:

```
ping 18.225.8.244
```

Saída:

```
Pinging 18.225.8.244 with 32 bytes of data:

Request timed out.
```

Observe que o ping falha e que o tráfego está bloqueado.

2. Use o endereço IPv4 privado para se conectar e verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Saída:

```
The authenticity of host '10.0.1.85' can't be established.
ECDSA key fingerprint is SHA256:3zo/gSss+HAZ+7eTyWlOB/Ke04IM+hadjsoLJeRTWBk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.1.85' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
```

```
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
/ /
/m/'
Last login: Fri Sep 27 14:16:53 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Observe que o ping falha e que o tráfego está bloqueado.

3. Emita um ping para a instância B usando o endereço IPv4 público para verificar se há tráfego de entrada:

```
ping 3.18.106.198
```

Saída:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Observe que o ping falha e que o tráfego está bloqueado.

4. Use o endereço IPv4 privado para se conectar e verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id  i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

Saída:

```
The authenticity of host '10.0.2.98' can't be established.
ECDSA key fingerprint is SHA256:0IjXKKyVlDthcCfI0IPIJMUiItAOLYKRNLGTYURnFXo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.98' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
```

```
~~..   _/
/ /
/m/'
Last login: Fri Sep 27 14:18:16 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Observe que o ping falha e que o tráfego está bloqueado.

5. Conecte-se à instância C. Como não há endereço IP público para o qual emitir um ping, use o EC2 Instance Connect para se conectar e depois emita um ping da instância para um IP público para verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Saída:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
/ /
/m/'
Last login: Tue Sep 24 15:17:56 2024 from 10.0.2.86
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Observe que o ping falha e que o tráfego está bloqueado.

6. Conecte-se à instância D. Como não há endereço IP público para o qual emitir um ping, use o EC2 Instance Connect para se conectar e depois emita um ping da instância para um IP público para verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Saída:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ _/
_/m/'
Last login: Fri Sep 27 16:42:01 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:8200:7:49a5:5fd4:b121
 (2600:9000:25f3:8200:7:49a5:5fd4:b121)) 56 data bytes
```

Observe que o ping falha e que o tráfego está bloqueado.

2.3 Opcional: verificar se a conectividade está bloqueada com o Analisador de Acesso

O Analisador de Acessibilidade da VPC pode ser usado para entender se determinados caminhos de rede podem ou não ser acessados de acordo com sua configuração de rede, incluindo as configurações do BPA da VPC. Neste exemplo, você analisará o mesmo caminho de rede que foi tentado anteriormente para confirmar que o BPA da VPC é o motivo da falha de conectividade.

AWS Management Console

1. Vá para o console do Network Insights em https://console.aws.amazon.com/networkinsights/home#ReachabilityAnalyzer.
2. Clique em Criar e analisar caminho.
3. Em Tipo de origem, escolha Gateways da Internet e selecione o gateway da Internet marcado como Gateway da Internet do BPA da VPC na lista suspensa Origem.
4. Em Tipo de destino, escolha Instâncias e selecione a instância marcada com Instância A do BPA da VCP no menu suspenso Destino.
5. Clique em Criar e analisar caminho.
6. Aguarde a conclusão da análise. Pode levar alguns minutos.

7. Depois da conclusão, você deverá ver que o Status de acessibilidade é Não acessível e que Detalhes do caminho mostra que `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` é a causa.

AWS CLI

1. Crie um caminho de rede usando o ID do gateway da Internet marcado como Gateway da Internet do BPA da VPC e o ID da instância marcada como Instância A do BPA da VPC:

```
aws ec2 --region us-east-2 create-network-insights-path --source igw-id --
destination instance-id --protocol TCP
```

2. Inicie uma análise no caminho da rede:

```
aws ec2 --region us-east-2 start-network-insights-analysis --network-insights-
path-id nip-id
```

3. Recupere os resultados da análise:

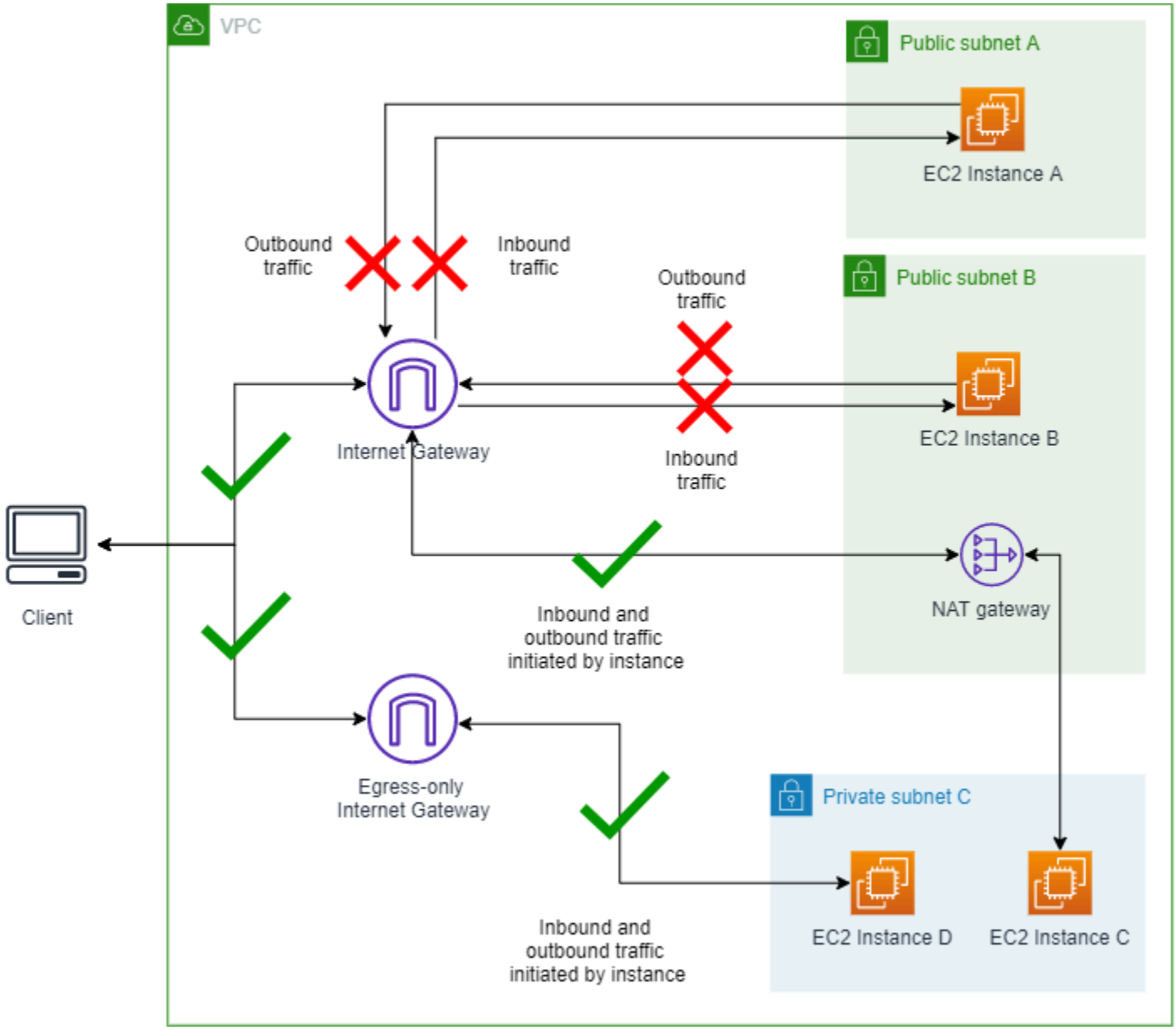
```
aws ec2 --region us-east-2 describe-network-insights-analyses --network-
insights-analysis-ids nia-id
```

4. Verifique se `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` é o `ExplanationCode` para a falta de acessibilidade.

Cenário 3: modificar o modo do BPA

Nesta seção, você alterará a direção do tráfego do BPA da VPC e só permitirá tráfego que use um gateway NAT ou um gateway da Internet somente de saída.

Diagrama do modo somente de entrada do BPA da VPC ativado:



3.1 Alterar o modo para somente de entrada

Conclua esta seção para alterar o modo.

AWS Management Console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação esquerdo, escolha Configurações.
3. Na guia Bloquear acesso público, escolha Editar configurações de acesso público.

4. Modifique as configurações do acesso público no console da VPC e altere a direção para Somente de entrada.
5. Salve as alterações e aguarde a atualização do status. Pode demorar alguns minutos para as configurações do BPA terem efeito e o status ser atualizado.

AWS CLI

1. Modifique o modo do BPA da VPC:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-
gateway-block-mode block-ingress
```

   Pode demorar alguns minutos para as configurações do BPA terem efeito e o status ser atualizado.
2. Visualize o status do BPA da VPC:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

3.2 Conectar-se a instâncias

Conclua esta seção para se conectar às instâncias.

AWS Management Console

1. Emita um ping para o endereço IPv4 público da instância A e da instância B, como fez no cenário 1. Observe que o tráfego está bloqueado.
2. Conecte-se à instância A e à instância B usando o EC2 Instance Connect, como fez no cenário 1 e emita um ping das instâncias para www.amazon.com. Observe que você não pode emitir ping da instância A ou B para um site público na Internet e que o tráfego está bloqueado.
3. Conecte-se à instância C e à instância D usando o EC2 Instance Connect, como fez no cenário 1 e emita um ping das instâncias para www.amazon.com. Observe que você pode emitir ping da instância C ou D para um site público na Internet e que o tráfego está permitido.

AWS CLI

1. Emita um ping para a instância A usando o endereço IPv4 público para verificar se há tráfego de entrada:

```
ping 18.225.8.244
```

Saída:

```
Pinging 18.225.8.244 with 32 bytes of data:

Request timed out.
```

Observe que o ping falha e que o tráfego está bloqueado.

2. Use o endereço IPv4 privado para se conectar e verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Saída:

```
The authenticity of host '10.0.1.85' can't be established.
ECDSA key fingerprint is SHA256:3zo/gSss+HAZ+7eTyWlOB/Ke04IM+hadjsoLJeRTWBk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.1.85' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
/ /
/m/'
Last login: Fri Sep 27 14:16:53 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Observe que o ping falha e que o tráfego está bloqueado.

3. Emita um ping para a instância B usando o endereço IPv4 público para verificar se há tráfego de entrada:

```
ping 3.18.106.198
```

Saída:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Observe que o ping falha e que o tráfego está bloqueado.

4. Use o endereço IPv4 privado para se conectar e verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

Saída:

```
The authenticity of host '10.0.2.98 ' can't be established.
ECDSA key fingerprint is SHA256:0IjXKKyVlDthcCfI0IPIJMUiItAOLYKRNLGTYURnFXo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.98' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ /
/m/'
Last login: Fri Sep 27 14:18:16 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Observe que o ping falha e que o tráfego está bloqueado.

5. Conecte-se à instância C. Como não há endereço IP público para o qual emitir um ping, use o EC2 Instance Connect para se conectar e depois emita um ping da instância para um IP público para verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Saída:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'

Last login: Tue Sep 24 15:28:09 2024 from 10.0.2.86

[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com

PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.

64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=248 time=1.84 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=248 time=1.40 ms
```

Observe que o ping foi bem-sucedido e o tráfego não está bloqueado.

6. Conecte-se à instância D. Como não há endereço IP público para o qual emitir um ping, use o EC2 Instance Connect para se conectar e depois emita um ping da instância para um IP público para verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Saída:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 16:48:38 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:5800:7:49a5:5fd4:b121
 (2600:9000:25f3:5800:7:49a5:5fd4:b121)) 56 data bytes
64 bytes from 2600:9000:25f3:5800:7:49a5:5fd4:b121
 (2600:9000:25f3:5800:7:49a5:5fd4:b121): icmp_seq=14 ttl=58 time=1.47 ms
64 bytes from 2600:9000:25f3:5800:7:49a5:5fd4:b121
 (2600:9000:25f3:5800:7:49a5:5fd4:b121): icmp_seq=16 ttl=58 time=1.59 ms
```

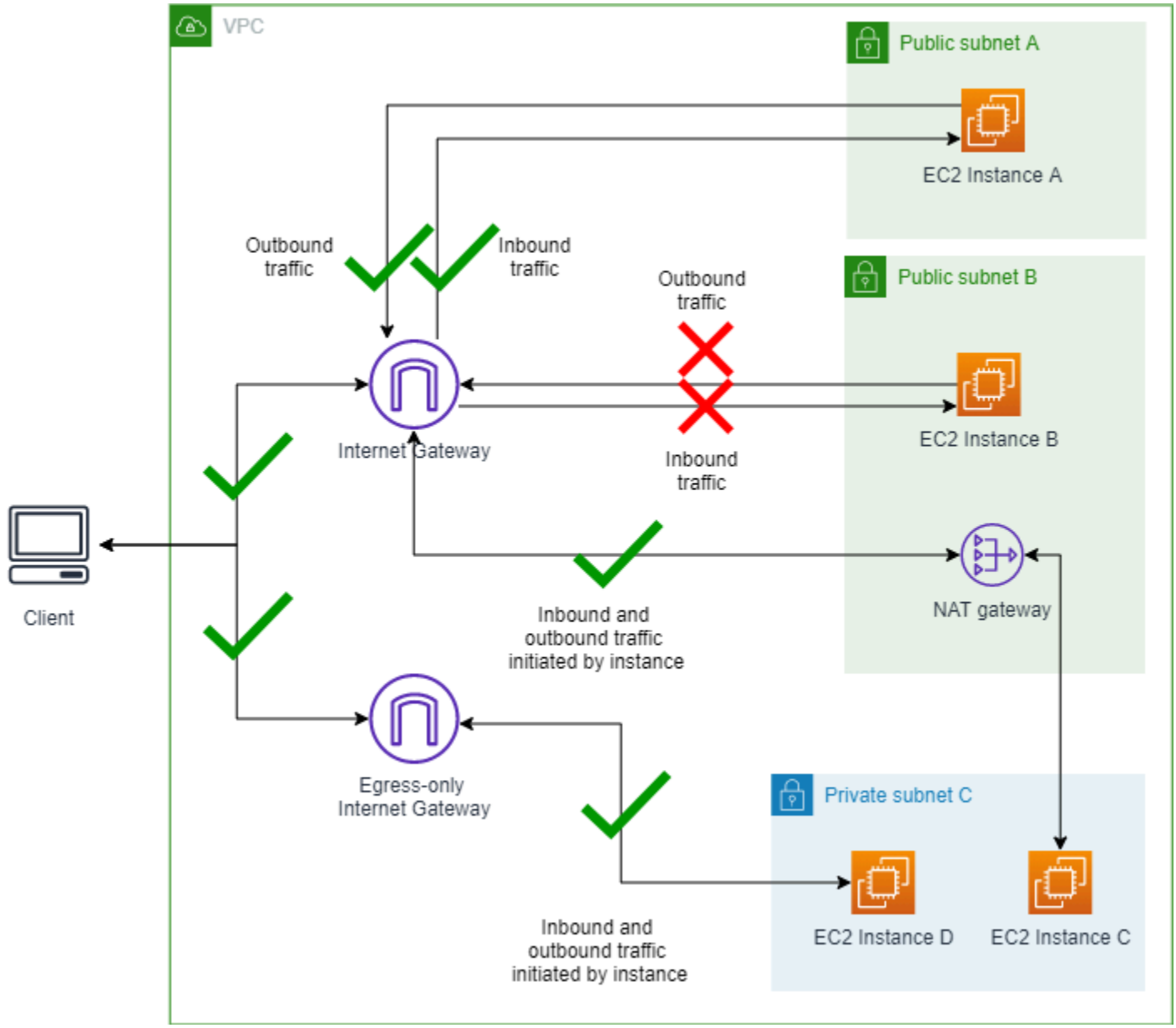
Observe que o ping foi bem-sucedido e o tráfego não está bloqueado.

Cenário 4: criar uma exclusão

Nesta seção, você criará uma exclusão e só bloqueará tráfego de e para a sub-rede que não esteja excluído do BPA da VPC. A exclusão do BPA da VPC é um modo que pode ser aplicado a uma única VPC ou sub-rede que a isenta do modo BPA da conta e permite acesso bidirecional ou somente de saída. Você pode criar exclusões do BPA para VPCs e sub-redes mesmo quando o BPA não está habilitado na conta para garantir que não haja interrupção do tráfego para as exclusões quando o BPA da VPC estiver ativado.

Neste exemplo, criaremos uma exclusão para a sub-rede A para mostrar como o tráfego para as exclusões é afetado pelo BPA da VPC.

Diagrama do modo somente de entrada do BPA da VPC ativado e da exclusão da sub-rede A com o modo bidirecional ativado:



4.1 Criar uma exclusão para a sub-rede A

Conclua esta seção para criar uma exclusão. A exclusão do BPA da VPC é um modo que pode ser aplicado a uma única VPC ou sub-rede que a isenta do modo BPA da conta e permite acesso bidirecional ou somente de saída. Você pode criar exclusões do BPA para VPCs e sub-redes mesmo quando o BPA não está habilitado na conta para garantir que não haja interrupção do tráfego para as exclusões quando o BPA da VPC estiver ativado.

AWS Management Console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.

2. No painel de navegação esquerdo, escolha Configurações.
3. Na guia Bloquear o acesso público, em Exclusões, escolha Criar exclusões.
4. Escolha Sub-rede pública A do BPA da VPC, certifique-se de que a direção de permissão Bidirecional esteja selecionada e escolha Criar exclusões.
5. Aguarde até que o status de Exclusão mude para Ativo. Pode ser necessário atualizar a tabela de exclusão para ver a alteração.

A exclusão foi criada.

AWS CLI

1. Modifique a direção de permissão da exclusão:

```
aws ec2 --region us-east-2 create-vpc-block-public-access-exclusion --subnet-
id subnet-id --internet-gateway-exclusion-mode allow-bidirectional
```

2. Pode levar algum tempo para o status da exclusão ser atualizado. Para visualizar o status da exclusão:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusions --
exclusion-ids exclusion-id
```

4.2 Conectar-se a instâncias

Conclua esta seção para se conectar às instâncias.

AWS Management Console

1. Emita um ping para o endereço IPv4 público da instância A. Observe que o tráfego está permitido.
2. Emita um ping para o endereço IPv4 público da instância B. Observe que o tráfego está bloqueado.
3. Conecte-se à instância A usando o EC2 Instance Connect, como fez no cenário 1 emita um ping para www.amazon.com. Observe que você pode emitir um ping da instância A para um site público na Internet e que o tráfego está permitido.

4. Conecte-se à instância B usando o EC2 instance Connect, como fez no cenário 1 emita um ping para www.amazon.com. Observe que você não pode emitir um ping da instância B para um site público na Internet. O tráfego está bloqueado.
5. Conecte-se à instância C e à instância D usando o EC2 Instance Connect, como fez no cenário 1 e emita um ping das instâncias para www.amazon.com. Observe que você pode emitir ping da instância C ou D para um site público na Internet. O tráfego está permitido.

AWS CLI

1. Emita um ping para a instância A usando o endereço IPv4 público para verificar se há tráfego de entrada:

```
ping 18.225.8.244
```

Saída:

```
Pinging 18.225.8.244 with 32 bytes of data:

Reply from 18.225.8.244: bytes=32 time=51ms TTL=110
Reply from 18.225.8.244: bytes=32 time=61ms TTL=110
```

Observe que o ping foi bem-sucedido e o tráfego não está bloqueado.

2. Use o endereço IPv4 privado para se conectar e verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Saída:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
/ /
```

```
/m/'
Last login: Fri Sep 27 17:58:12 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=249 time=1.03 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=249 time=1.72 ms
```

Observe que o ping foi bem-sucedido e o tráfego não está bloqueado.

3. Emita um ping para a instância B usando o endereço IPv4 público para verificar se há tráfego de entrada:

```
ping 3.18.106.198
```

Saída:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Observe que o ping falha e que o tráfego está bloqueado.

4. Use o endereço IPv4 privado para se conectar e verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

Saída:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ /
/m/'
Last login: Fri Sep 27 18:12:03 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
```

```
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Observe que o ping falha e que o tráfego está bloqueado.

5. Conecte-se à instância C. Como não há endereço IP público para o qual emitir um ping, use o EC2 Instance Connect para se conectar e depois emita um ping da instância para um IP público para verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Saída

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ /
/m/'

Last login: Tue Sep 24 15:28:09 2024 from 10.0.2.86

[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com

PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.

64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=248 time=1.84 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=248 time=1.40 ms
```

Observe que o ping foi bem-sucedido e o tráfego não está bloqueado.

6. Conecte-se à instância D. Como não há endereço IP público para o qual emitir um ping, use o EC2 Instance Connect para se conectar e depois emita um ping da instância para um IP público para verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Saída

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:00:52 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING
 www.amazon.com(g2600-141f-4000-059a-0000-0000-0000-3bd4.deploy.static.akamaitechnologie
 (2600:141f:4000:59a::3bd4)) 56 data bytes
64 bytes from
 g2600-141f-4000-059a-0000-0000-0000-3bd4.deploy.static.akamaitechnologies.com
 (2600:141f:4000:59a::3bd4): icmp_seq=1 ttl=48 time=15.9 ms
64 bytes from
 g2600-141f-4000-059a-0000-0000-0000-3bd4.deploy.static.akamaitechnologies.com
 (2600:141f:4000:59a::3bd4): icmp_seq=2 ttl=48 time=15.8 ms
```

Observe que o ping foi bem-sucedido e o tráfego não está bloqueado.

4.3 Opcional: verificar a conectividade com o Analisador de Acessibilidade

Usando o mesmo caminho de rede criado no Analisador de Acessibilidade no cenário 2, você agora pode executar uma nova análise e confirmar se o caminho está acessível agora que uma exclusão foi criada para a sub-rede pública A.

Para obter informações sobre a disponibilidade regional do Analisador de Acessibilidade, consulte Considerations no Reachability Analyzer Guide.

AWS Management Console

1. No caminho de rede que você criou anteriormente no console do Network Insights, clique em Executar novamente a análise.
2. Aguarde a conclusão da análise. Isso pode demorar muitos minutos.
3. Confirme se o caminho agora está Acessível.

AWS CLI

1. Usando o ID do caminho de rede criado anteriormente, inicie uma nova análise:

```
aws ec2 --region us-east-2 start-network-insights-analysis --network-insights-path-id nip-id
```

2. Recupere os resultados da análise:

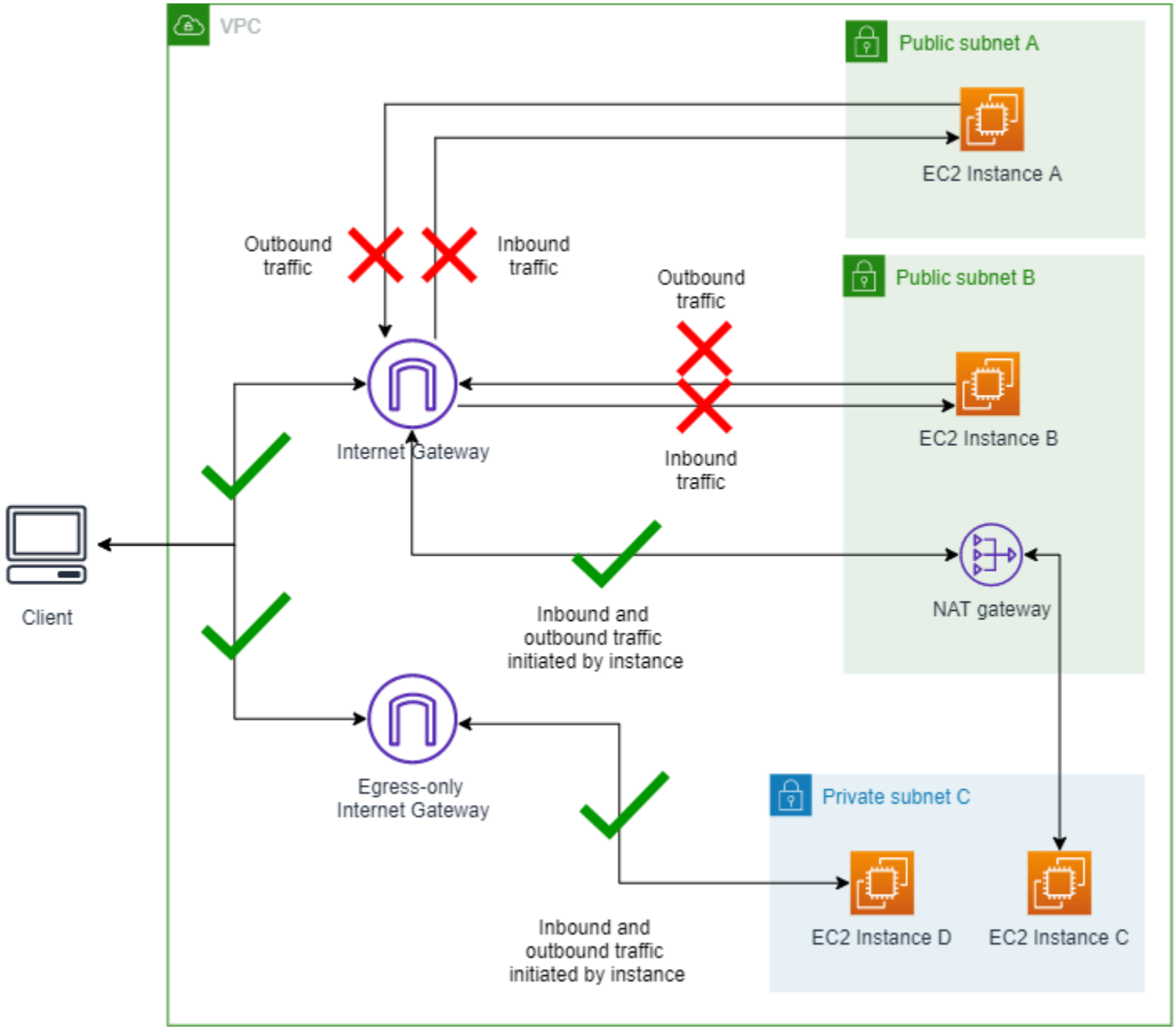
```
aws ec2 --region us-east-2 describe-network-insights-analyses --network-insights-analysis-ids nia-id
```

3. Confirme se o código de explicação `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` não ocorre mais.

Cenário 5: modificar o modo de exclusão

Nesta seção, você alterará a direção de tráfego permitida na exclusão para ver como isso afeta o BPA da VPC. Observe que o modo somente de saída para uma exclusão não é realmente significativo com o BPA da VPC ativado no modo Bloquear somente de entrada. Esse é do mesmo comportamento do cenário 3.

Diagrama do modo somente de entrada do BPA da VPC ativado e da exclusão da sub-rede A com o modo somente de saída ativado:



5.1 Alterar a direção de permissão da exclusão para somente de saída

Conclua esta seção para alterar a direção de permissão da exclusão.

AWS Management Console

1. Edite a exclusão que você criou no cenário 4 e altere a direção de permissão para Somente de saída.
2. Escolha Salvar alterações.

3. Aguarde até que o status de Exclusão mude para Ativo. Pode demorar alguns minutos para as configurações do BPA terem efeito e o status ser atualizado. Pode ser necessário atualizar a tabela de exclusão para ver a alteração.

AWS CLI

1. Modifique a direção de permissão da exclusão:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-exclusion --exclusion-
id exclusion-id --internet-gateway-exclusion-mode allow-egress
```

   Pode demorar alguns minutos para as configurações do BPA terem efeito e o status ser atualizado.
2. Pode levar algum tempo para o status da exclusão ser atualizado. Para visualizar o status da exclusão:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusion
```

5.2 Conectar-se a instâncias

Conclua esta seção para se conectar às instâncias.

AWS Management Console

1. Emita um ping para o endereço IPv4 público da instância A e da instância B. Observe que o tráfego está bloqueado.
2. Conecte-se à instância A e à instância B usando o EC2 Instance Connect, como fez no cenário 1 emita um ping para www.amazon.com. Observe que você não pode emitir um ping da instância A ou B para um site público na Internet. O tráfego está bloqueado.
3. Conecte-se à instância C e à instância D usando o EC2 Instance Connect, como fez no cenário 1 e emita um ping das instâncias para www.amazon.com. Observe que você pode emitir ping da instância C ou D para um site público na Internet. O tráfego está permitido.

AWS CLI

1. Emita um ping para a instância A usando o endereço IPv4 público para verificar se há tráfego de entrada:

```
ping 18.225.8.244
```

Saída:

```
Pinging 18.225.8.244 with 32 bytes of data:
Request timed out.
```

Observe que o ping falha e que o tráfego está bloqueado.

2. Use o endereço IPv4 privado para se conectar e verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Saída:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:09:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Observe que o ping falha e que o tráfego está bloqueado.

3. Emita um ping para a instância B usando o endereço IPv4 público para verificar se há tráfego de entrada:

```
ping 3.18.106.198
```

Saída:

```
Pinging 3.18.106.198 with 32 bytes of data:
```

```
Request timed out.
```

Observe que o ping falha e que o tráfego está bloqueado.

4. Use o endereço IPv4 privado para se conectar e verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Saída:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:09:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Observe que o ping falha e que o tráfego está bloqueado.

5. Conecte-se à instância C. Como não há endereço IP público para o qual emitir um ping, use o EC2 Instance Connect para se conectar e depois emita um ping da instância para um IP público para verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Saída:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
```

```
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:00:31 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:a600:7:49a5:5fd4:b121
 (2600:9000:25f3:a600:7:49a5:5fd4:b121)) 56 data bytes
64 bytes from 2600:9000:25f3:a600:7:49a5:5fd4:b121
 (2600:9000:25f3:a600:7:49a5:5fd4:b121): icmp_seq=1 ttl=58 time=1.51 ms
64 bytes from 2600:9000:25f3:a600:7:49a5:5fd4:b121
 (2600:9000:25f3:a600:7:49a5:5fd4:b121): icmp_seq=2 ttl=58 time=1.49 ms
```

Observe que o ping foi bem-sucedido e o tráfego não está bloqueado.

6. Conecte-se à instância D. Como não há endereço IP público para o qual emitir um ping, use o EC2 Instance Connect para se conectar e depois emita um ping da instância para um IP público para verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Saída:

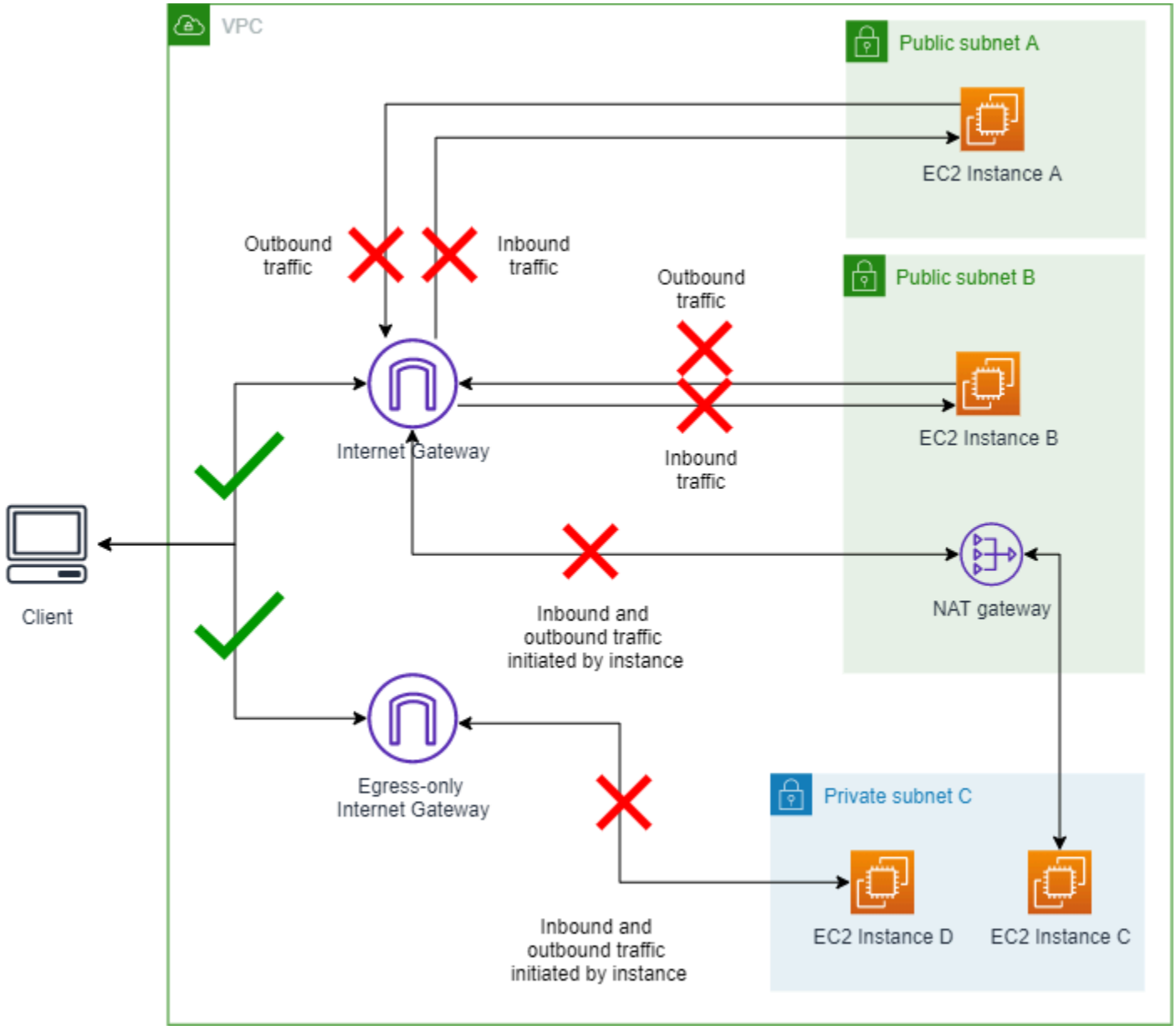
```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:13:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2606:2cc0::374 (2606:2cc0::374)) 56 data bytes
64 bytes from 2606:2cc0::374 (2606:2cc0::374): icmp_seq=1 ttl=58 time=1.21 ms
64 bytes from 2606:2cc0::374 (2606:2cc0::374): icmp_seq=2 ttl=58 time=1.51 ms
```

Observe que o ping foi bem-sucedido e o tráfego não está bloqueado.

Cenário 6: modificar o modo do BPA

Nesta seção, você alterará a direção de bloqueio do BPA da VPC para ver como isso afeta o tráfego. Neste cenário, o BPA da VPC habilitado no modo bidirecional bloqueia todo o tráfego exatamente como no cenário 1. A menos que uma exclusão tenha acesso a um gateway NAT ou um gateway da Internet somente de saída, o tráfego estará bloqueado.

Diagrama do modo bidirecional do BPA da VPC ativado e da exclusão da sub-rede A com o modo somente de saída ativado:



6.1 Alterar o BPA da VPC para o modo bidirecional

Conclua esta seção para alterar o modo do BPA.

AWS Management Console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação esquerdo, escolha Configurações.
3. Escolha Editar configurações de acesso público.
4. Altere a direção do bloqueio para Bidirecional e escolha Salvar alterações.
5. Aguarde até que Status mude para Ativado. Pode demorar alguns minutos para as configurações do BPA terem efeito e o status ser atualizado.

AWS CLI

1. Modifique a direção do bloqueio do BPA da VPC:

   ```
   aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-gateway-block-mode block-bidirectional
   ```

   Pode demorar alguns minutos para as configurações do BPA terem efeito e o status ser atualizado.
2. Visualize o status do BPA da VPC:

   ```
   aws ec2 --region us-east-2 describe-vpc-block-public-access-options
   ```

6.2 Conectar-se a instâncias

Conclua esta seção para se conectar às instâncias.

AWS Management Console

1. Emita um ping para o endereço IPv4 público da instância A e da instância B. Observe que o tráfego está bloqueado.
2. Conecte-se à instância A e à instância B usando o EC2 Instance Connect, como fez no cenário 1 emita um ping para www.amazon.com. Observe que você não pode emitir um ping da instância A ou B para um site público na Internet. O tráfego está bloqueado.

3. Conecte-se à instância C e à instância D usando o EC2 Instance Connect, como fez no cenário 1 e emita um ping das instâncias para www.amazon.com. Observe que você não pode emitir ping da instância C ou D para um site público na Internet. O tráfego está bloqueado.

AWS CLI

1. Emita um ping para a instância A usando o endereço IPv4 público para verificar se há tráfego de entrada:

```
ping 18.225.8.244
```

Saída:

```
Pinging 18.225.8.244 with 32 bytes of data:
Request timed out.
```

Observe que o ping falha e que o tráfego está bloqueado.

2. Use o endereço IPv4 privado para se conectar e verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Saída:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:17:44 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Observe que o ping falha e que o tráfego está bloqueado.

3. Emita um ping para a instância A usando o endereço IPv4 público para verificar se há tráfego de entrada:

```
ping 3.18.106.198
```

Saída:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Observe que o ping falha e que o tráfego está bloqueado.

4. Use o endereço IPv4 privado para se conectar e verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Saída:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:09:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Observe que o ping falha e que o tráfego está bloqueado.

5. Conecte-se à instância C. Como não há endereço IP público para o qual emitir um ping, use o EC2 Instance Connect para se conectar e depois emita um ping da instância para um IP público para verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Saída:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:19:45 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:6200:7:49a5:5fd4:b121
 (2600:9000:25f3:6200:7:49a5:5fd4:b121)) 56 data bytes
```

Observe que o ping falha e que o tráfego está bloqueado.

6. Conecte-se à instância D. Como não há endereço IP público para o qual emitir um ping, use o EC2 Instance Connect para se conectar e depois emita um ping da instância para um IP público para verificar se há tráfego de saída:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Saída:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
```

```
Last login: Fri Sep 27 18:20:58 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:b400:7:49a5:5fd4:b121
 (2600:9000:25f3:b400:7:49a5:5fd4:b121)) 56 data bytes
```

Observe que o ping falha e que o tráfego está bloqueado.

Limpeza

Nesta seção, você excluirá todos os recursos que criou para este exemplo avançado. É importante limpar os recursos para evitar cobranças adicionais excessivas pelos recursos criados em sua conta.

Excluir os recursos do CloudFormation

Conclua esta seção para excluir os recursos que você criou com o modelo do AWS CloudFormation.

AWS Management Console

1. Abra o console do AWS CloudFormation em https://console.aws.amazon.com/cloudformation/.
2. Escolha a pilha do BPA da VPC.
3. Escolha Excluir.
4. Depois que começar a excluir a pilha, na guia Eventos, visualize o andamento e certifique-se de que a pilha seja excluída. Talvez seja necessário forçar a exclusão da pilha para que ela seja totalmente excluída.

AWS CLI

1. Excluir a pilha do CloudFormation. Talvez seja necessário forçar a exclusão da pilha para que ela seja totalmente excluída.

```
aws cloudformation delete-stack --stack-name VPC-BPA-stack --region us-east-2
```

2. Visualize o andamento e certifique-se de que a pilha seja excluída.

```
aws cloudformation describe-stack-events --stack-name VPC-BPA-stack --region us-east-2
```

Rastrear a remoção de exclusões com o AWS CloudTrail

Conclua esta seção para rastrear a remoção de exclusões com o AWS CloudTrail. As entradas do CloudTrail aparecem quando você remove uma exclusão.

AWS Management Console

Você pode visualizar todas as exclusões removidas no histórico de eventos do CloudTrail consultando Tipo de recurso > AWS::EC2::VPCBlockPublicAccessExclusion no console do AWS CloudTrail em https://console.aws.amazon.com/cloudtrailv2/.

AWS CLI

Você pode usar o comando lookup-events para visualizar os eventos relacionados com remoção de exclusões:

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceType,AttributeValue=AWS::EC2::VPCBlockPublicAccessExclusion
```

O exemplo avançado foi concluído.

Melhores práticas de segurança para a VPC

As práticas recomendadas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas práticas recomendadas podem não ser adequadas ou suficientes para o seu ambiente, trate-as como considerações úteis em vez de prescrições.

- Quando você adicionar sub-redes à VPC para hospedar seu aplicativo, crie-as em várias zonas de disponibilidade. Uma zona de disponibilidade é um ou mais data centers discretos com energia, redes e conectividade redundantes em uma região da AWS. O uso de várias zonas de disponibilidade torna os aplicativos em produção altamente disponíveis, tolerantes a falhas e escaláveis.
- Use grupos de segurança para controlar o tráfego para instâncias do EC2 em suas sub-redes. Para ter mais informações, consulte Grupos de segurança.
- Use ACLs de rede para controlar o tráfego de entrada e saída em nível de sub-rede. Para ter mais informações, consulte Controlar o tráfego da sub-rede com listas de controle de acesso à rede.
- Gerencie o acesso aos recursos da AWS na sua VPC usando federação de identidades, usuários e perfis do AWS Identity and Access Management (IAM). Para ter mais informações, consulte Identity and Access Management para o Amazon VPC.

- Utilize o VPC Flow Logs para monitorar o tráfego de IP de e para uma VPC, sub-rede ou interface de rede. Para ter mais informações, consulte VPC Flow Logs.
- Use o Analisador de Acesso à Rede para identificar o acesso não intencional da rede aos recursos em nossas VPCs. Para obter mais informações, consulte o Guia do Analisador de Acesso à Rede.
- Use o AWS Network Firewall para monitorar e proteger sua VPC filtrando o tráfego de entrada e saída. Para obter mais informações, consulte o Guia do AWS Network Firewall.
- Use o Amazon GuardDuty para detectar possíveis ameaças às suas contas, contêineres, workloads e dados no ambiente da AWS. A detecção básica de ameaças inclui o monitoramento dos logs de fluxo da VPC associados às instâncias do Amazon EC2. Para obter mais informações, consulte Logs de fluxo da VPC no Amazon GuardDuty User Guide.

Para obter respostas a perguntas frequentes relacionadas à segurança da VPC, consulte Segurança e filtragem, nas Perguntas frequentes sobre o Amazon VPC.

Usar a Amazon VPC com outros Serviços da AWS

A Amazon Virtual Private Cloud (VPC) é um serviço fundamental da AWS que fornece um ambiente de rede seguro e personalizável para sua infraestrutura de nuvem. Além de criar e gerenciar sua própria VPC, você pode aproveitar a integração entre a VPC e outros serviços da AWS para criar soluções abrangentes adaptadas às suas necessidades específicas.

Você pode conectar sua VPC a vários serviços da AWS usando o AWS PrivateLink. Isso torna possível a conectividade privada entre sua VPC e serviços da AWS ou aplicações on-premises compatíveis, mantendo o tráfego de rede dentro da rede da AWS e evitando a exposição à Internet pública. Isso é particularmente útil para manter limites de segurança e requisitos de conformidade mais rígidos.

Para fortalecer ainda mais a segurança da sua VPC, é possível usar o AWS Network Firewall. Esse serviço de firewall gerenciado permite definir e aplicar políticas de segurança em nível de rede, filtrando o tráfego norte-sul e leste-oeste em sua VPC. Ao emparelhar o Network Firewall com sua VPC, você pode aprimorar sua estratégia de defesa e proteger seus recursos de nuvem contra acesso não autorizado ou atividades maliciosas.

Além disso, você pode filtrar o tráfego DNS em sua VPC usando o Route 53 Resolver DNS Firewall. Esse recurso permite criar regras personalizadas de filtragem de DNS para controlar quais domínios seus recursos de VPC podem resolver, fornecendo uma camada adicional de segurança e fiscalização de conformidade.

Se encontrar problemas de acessibilidade entre recursos dentro da sua VPC ou conectados à sua VPC, você poderá usar o Reachability Analyzer. O Reachability Analyzer realiza testes de conectividade virtual, fornecendo informações detalhadas do caminho passo a passo e identificando quaisquer componentes de bloqueio. Essa ferramenta de solução de problemas pode ajudar a identificar e resolver rapidamente problemas de conectividade de rede.

Ao integrar esses serviços da AWS complementares à sua VPC, você poderá criar soluções de nuvem poderosas, seguras e resilientes que atendam aos seus requisitos exclusivos de negócios e arquitetura.

Conteúdo

- Filtrar o tráfego de DNS usando o Route 53 Resolver DNS Firewall
- Solucionar problemas de acessibilidade usando o Reachability Analyzer

Conectar sua VPC a outro serviços usando o AWS PrivateLink

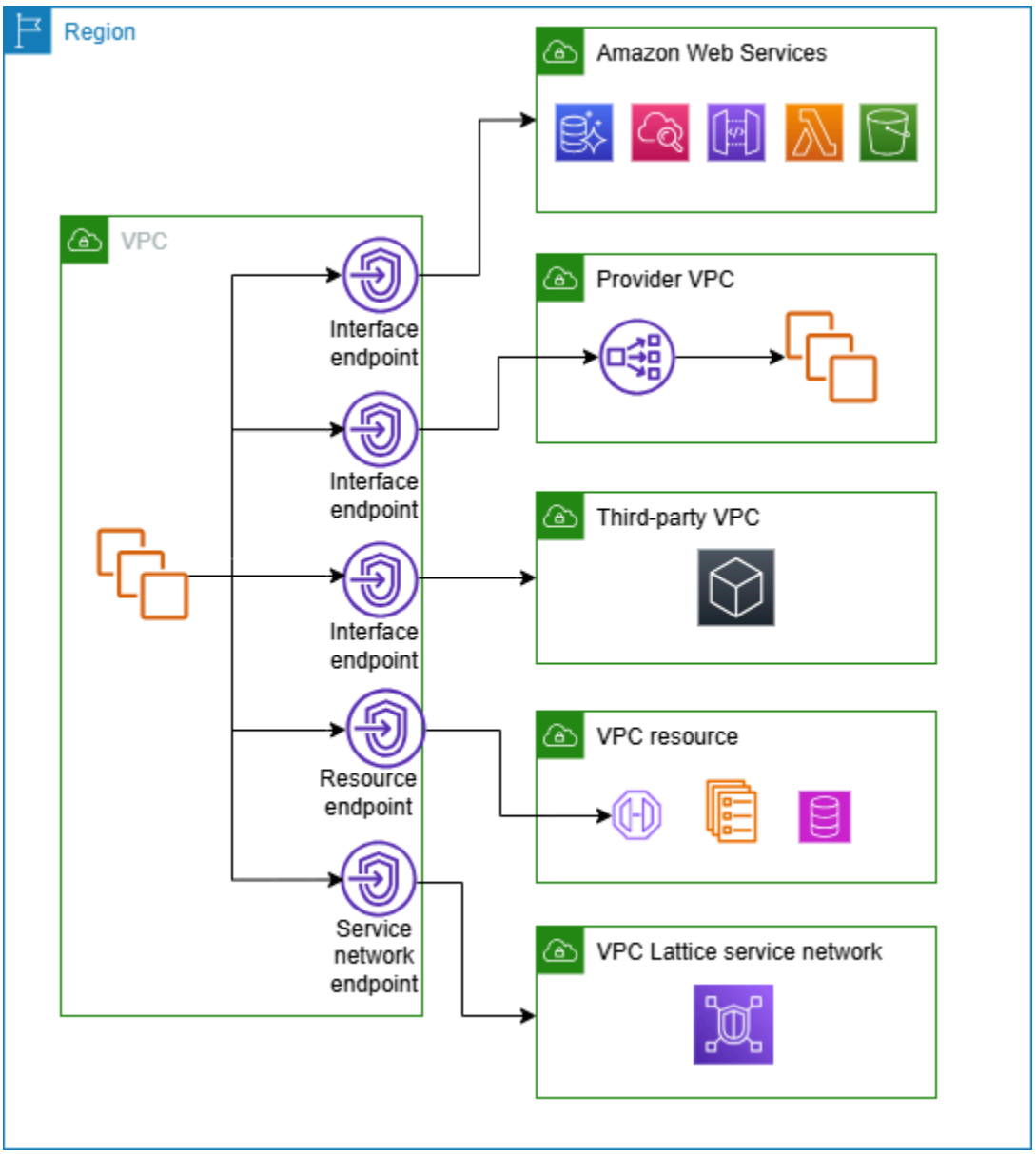
O AWS PrivateLink estabelece conectividade privada entre nuvens privadas virtuais (VPCs) e Serviços da AWS com suporte, serviços hospedados por outras contas da Contas da AWS, serviços do AWS Marketplace com suporte e recursos compatíveis. Não é necessário usar um gateway da Internet, um dispositivo NAT, uma conexão do AWS Direct Connect ou uma conexão do AWS Site-to-Site VPN para estabelecer comunicação com o serviço ou recurso.

Para usar o AWS PrivateLink, crie um endpoint da VPC em qualquer sub-rede da qual você precise acessar o serviço ou o recurso. Isso criará interfaces de rede elásticas nas sub-redes especificadas, que servirão como pontos de entrada para o tráfego destinado ao serviço ou ao recurso.

Você também pode criar seu próprio serviço de endpoint da VPC habilitado pelo AWS PrivateLink e permitir que outros clientes da AWS acessem o serviço. O PrivateLink permite a criação de endpoints de API privados, permitindo que as organizações exponham seus próprios serviços com segurança a outros clientes da AWS. Isso permite que as empresas monetizem suas capacidades internas, promovam ecossistemas colaborativos e mantenham o controle sobre como seus serviços são acessados e consumidos.

Um dos principais benefícios do uso do AWS PrivateLink é a capacidade de estabelecer conectividade segura e privada sem a necessidade de construções de rede tradicionais, como gateways da Internet, dispositivos NAT ou conexões VPN. Isso ajuda a simplificar a arquitetura da rede, reduzir a superfície de ataque e melhorar a segurança geral, mantendo o tráfego de dados confinado na rede da AWS.

O diagrama a seguir mostra casos de uso comuns para o AWS PrivateLink. A VPC contém várias instâncias do EC2 em uma sub-rede privada, que acessam os recursos por meio de cinco endpoints da VPC. Há três endpoints da VPC de interface, um endpoint da VPC de recurso e um endpoint da VPC de rede de serviço.



Para ter mais informações, consulte AWS PrivateLink.

Filtrar o tráfego de rede usando o AWS Network Firewall

Você pode filtrar o tráfego de rede no perímetro da VPC usando o AWS Network Firewall. O Network Firewall é um serviço gerenciado e de firewall de rede com estado para detecção e prevenção de intrusões. Para obter mais informações, consulte o Guia do desenvolvedor do AWS Network Firewall.

Implemente o Network Firewall com os seguintes recursos da AWS.

Recurso do Network Firewall	Descrição
Firewall	Um firewall conecta o comportamento de filtragem de tráfego de rede de uma política de firewall à VPC que você deseja proteger. A configuração do firewall inclui especificações para as zonas de disponibilidade e sub-redes em que os endpoints de firewall são colocados. Ela também define configurações de alto nível, como configuração de registro em log de firewall e marcação no recurso de firewall da AWS. Para obter mais informações, consulte Firewalls no AWS Network Firewall.
Política de firewall	Uma política de firewall define o comportamento de monitoramento e proteção de um firewall. Os detalhes do comportamento são definidos nos grupos de regras que você adiciona à política e em algumas configurações padrão de política. Para usar uma política de firewall, associe-a a um ou mais firewalls. Para obter mais informações, consulte Políticas de firewall no AWS Network Firewall.
Grupo de regras	Um grupo de regras é um conjunto reutilizável de critérios para inspecionar e lidar com o tráfego de rede. Você adiciona um ou mais grupos de regras a uma política de firewall como parte da configuração de política. Você pode definir grupos de regras sem estado para inspecionar cada pacote de rede isoladamente. Os grupos de regras sem estado são semelhantes em comportamento e são usados para access control lists (ACLs – listas de controle de acesso) à rede da Amazon VPC. Você pode igualmente definir grupos de regras com estado para inspecionar pacotes no contexto do fluxo de tráfego. Grupos de regras com estado são semelhantes em comportamento e são usados para grupos de segurança da Amazon VPC. Para obter mais informações sobre grupos de regras, consulte Regras de grupos em AWS Network Firewall.

Você também pode usar o AWS Firewall Manager para configurar e gerenciar centralmente os recursos do Network Firewall nas contas e aplicações no AWS Organizations. Você pode gerenciar firewalls para várias contas usando uma única conta no Firewall Manager. Para obter mais informações, consulte AWS Firewall Manager no Guia do desenvolvedor do AWS WAF, AWS Firewall Manager e AWS Shield Advanced.

Filtrar o tráfego de DNS usando o Route 53 Resolver DNS Firewall

Com o Firewall DNS, você define regras de filtragem de nomes de domínio em grupos de regras que você associa às VPCs. Você pode especificar listas de nomes de domínio para permitir ou bloquear e personalizar as respostas para as consultas DNS que você bloqueia. Para obter mais informações, consulte a Documentação do Firewall DNS Resolver Route 53.

Você implementa o DNS Firewall com os seguintes recursos da AWS.

Recurso do Firewall DNS	Descrição
Grupo de regras do Firewall DNS	Um grupo de regras do Firewall DNS é uma coleção nomeada e reutilizável de regras de Firewall DNS para filtrar consultas de DNS. Preencha o grupo de regras com as regras de filtragem e, em seguida, associe o grupo de regras a uma ou mais VPCs da Amazon VPC. Quando você associa um grupo de regras a uma VPC, você habilita a filtragem do Firewall DNS para a VPC. Em seguida, quando o Resolver recebe uma consulta de DNS para uma VPC que tenha um grupo de regras associado a ela, ele passa a consulta para o Firewall DNS para filtragem. Cada regra dentro do grupo de regras especifica uma lista de domínios e uma ação a ser executada em consultas de DNS cujos domínios correspondem às especificações de domínio na lista. Você pode permitir, bloquear ou alertar sobre consultas correspondentes. Você também pode definir respostas personalizadas para consultas bloqueadas. Para obter mais informações, consulteRule groups and rules in Route 53 Resolver DNS Firewall (Grupos de regras e regras no Firewall DNS do Resolver do Route 53).

Recurso do Firewall DNS	Descrição
Lista de domínios	Uma lista de domínios é um conjunto reutilizável de especificações de domínios que você usa em uma regra do DNS Firewall, dentro de um grupo de regras. Para obter mais informações, consulteDomain lists in Route 53 Resolver DNS Firewall (Listas de domínios no Firewall DNS do Resolver do Route 53).

Você também pode usar o AWS Firewall Manager para configurar e gerenciar centralmente os recursos do Firewall DNS em suas contas e organizações do AWS Organizations. Você pode gerenciar firewalls para várias contas usando uma única conta no Firewall Manager. Para obter mais informações, consulte AWS Firewall Manager no Guia do desenvolvedor do AWS WAF, AWS Firewall Manager e AWS Shield Advanced.

Solucionar problemas de acessibilidade usando o Reachability Analyzer

O Reachability Analyzer é uma ferramenta de análise de configuração estática. Use o Reachability Analyzer para analisar e depurar a acessibilidade da rede entre dois recursos em sua VPC. O Reachability Analyzer produz detalhes salto a salto do caminho virtual entre esses recursos quando eles estão acessíveis e identifica o componente responsável pelo bloqueio quando eles estão inacessíveis.

Você pode usar o Reachability Analyzer para analisar a acessibilidade entre os seguintes recursos:

- Instâncias
- Gateways da Internet
- Interfaces de rede
- Gateways de trânsito
- Anexos do gateway de trânsito
- Serviços do VPC endpoint
- Endpoints da VPC

- Conexões de emparelhamento da VPC
- Gateways de VPN

Para obter mais informações, consulte o Guia do Analisador de Acessabilidade.

Exemplos de VPC

A Amazon Virtual Private Cloud (VPC) é um alicerce fundamental dentro do ecossistema da AWS, permitindo a você provisionar redes virtuais isoladas adaptadas às suas necessidades específicas. Ao criar e gerenciar suas próprias VPCs, você obtém controle total sobre o ambiente de rede, incluindo a capacidade de definir intervalos de endereços IP, sub-redes, tabelas de roteamento e opções de conectividade.

Esta seção contém três exemplos de configurações para suas nuvens privadas virtuais (VPC), cada uma delas criada para atender a um conjunto diferente de requisitos:

- VPC para um ambiente de teste: essa configuração mostra como criar uma VPC que pode ser usada como ambiente de desenvolvimento ou teste.
- VPC para servidores Web e de banco de dados: essa configuração mostra como criar uma VPC que pode ser usada em uma arquitetura resiliente em um ambiente de produção.
- VPC com servidores em sub-redes privadas e NAT: nessa configuração mais avançada, todas as instâncias do EC2 são provisionadas em sub-redes privadas, com um gateway NAT que facilita o acesso seguro de saída para a Internet. Esse é um exemplo de situação em que você precisa limitar a conectividade direta com a Internet aos seus recursos e, ao mesmo tempo, ativar a comunicação de saída necessária.

Ao fornecer esses exemplos de configurações de VPC, esperamos ilustrar as opções de flexibilidade e personalização disponíveis ao projetar seu ambiente de rede em nuvem. A configuração específica de VPC que você escolher deve se basear na arquitetura, nos requisitos de segurança e nos objetivos gerais de negócios da sua aplicação. Planejar cuidadosamente sua infraestrutura de VPC pode ajudar a criar uma rede virtual robusta, escalável e segura capaz de acomodar o crescimento e a evolução das suas workloads baseadas na nuvem.

Exemplos

Exemplos relacionados

- Para conectar suas VPCs umas às outras, consulte Configurações de emparelhamento de VPCs no Guia de emparelhamento da Amazon VPC.
- Para estabelecer conexão entre as VPCs e a própria rede, consulte Site-to-Site VPN scenarios no Guia do usuário do AWS Site-to-Site VPN.
- Para estabelecer conexão entre as VPCs e a própria rede, consulte Example transit gateway scenarios no Amazon VPC Transit Gateways.

Recursos adicionais

- Entenda os padrões de resiliência e as compensações (Blog de arquitetura da AWS)
- Planeje sua topologia de rede (AWS Well-Architected Framework)
- Opções de conectividade da Amazon Virtual Private Cloud (whitepapers da AWS)

Exemplo: VPC para um ambiente de teste

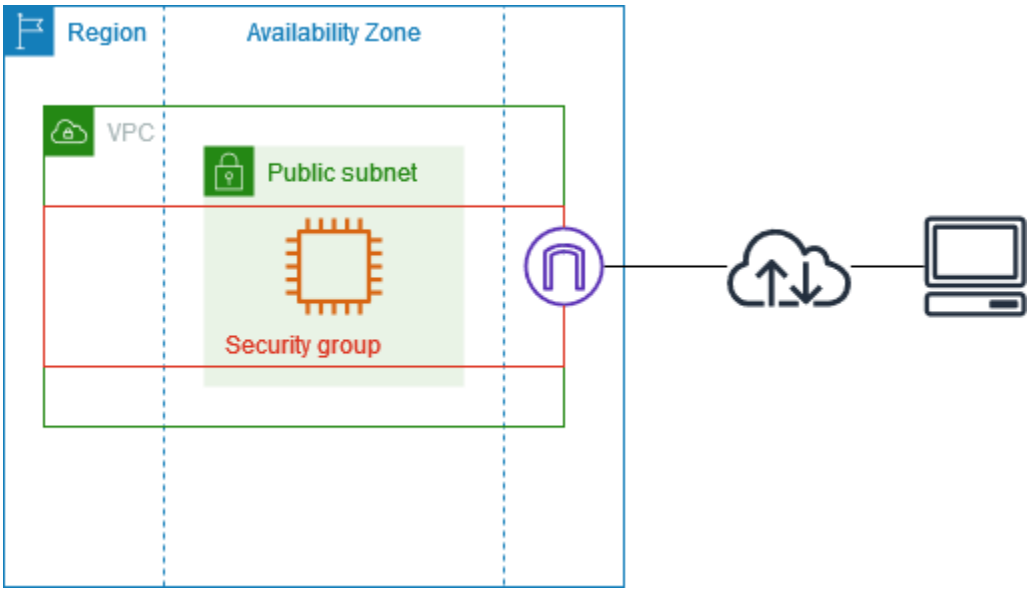
Este exemplo demonstra como criar uma VPC que pode ser usada como ambiente de desenvolvimento ou teste. Como essa VPC não se destina a ser usada na produção, não é necessário implantar seus servidores em várias zonas de disponibilidade. Para manter o custo e a complexidade baixos, você pode implantar os seus servidores em uma única zona de disponibilidade.

Conteúdo

Visão geral

O diagrama a seguir fornece uma visão geral dos recursos incluídos neste exemplo. A VPC tem uma sub-rede pública em uma única zona de disponibilidade e um gateway da Internet. O servidor é uma instância do EC2 executada na sub-rede pública. O grupo de segurança da instância permite o

tráfego SSH do seu próprio computador, além de qualquer outro tráfego especificamente necessário para suas atividades de desenvolvimento ou teste.



Roteamento

Quando essa VPC é criada usando o console da Amazon VPC, criamos uma tabela de rotas para a sub-rede pública com rotas locais e rotas para o gateway da Internet. Veja a seguir um exemplo da tabela de rotas com rotas para IPv4 e IPv6. Se você criar uma sub-rede somente IPv4 em vez de uma sub-rede de pilha dupla, sua tabela de rotas terá somente as rotas IPv4.

Destino	Destino
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
0.0.0.0/0	*igw-id*
::/0	*igw-id*

Segurança

Para este exemplo de configuração, é necessário criar um grupo de segurança para sua instância que permita o tráfego de que sua aplicação precisa. Por exemplo, talvez seja necessário adicionar uma regra que permita o tráfego SSH do seu computador ou o tráfego HTTP da sua rede.

Os exemplos a seguir demonstram regras de entrada para um grupo de segurança com regras para IPv4 e IPv6. Se você criar sub-redes somente IPv4 em vez de sub-redes de pilha dupla, serão necessárias apenas as regras para IPv4.

Origem	Protocolo	Intervalo de portas	Descrição
0.0.0.0/0	TCP	80	Permite acesso HTTP de entrada de todos os endereços IPv4
::/0	TCP	80	Permite acesso HTTP de entrada de todos os endereços IPv6
0.0.0.0/0	TCP	443	Permite acesso HTTPS de entrada de todos os endereços IPv4
::/0	TCP	443	Permite acesso HTTPS de entrada de todos os endereços IPv6
Intervalo de endereços IPv4 públicos da sua rede	TCP	22	(Opcional) Permite acesso SSH de entrada de endereços IP IPv4 na sua rede
Intervalo de endereços IPv6 da sua rede	TCP	22	(Opcional) Permite acesso SSH de entrada de endereços IP IPv6 na sua rede
Intervalo de endereços IPv4 públicos da sua rede	TCP	3389	(Opcional) Permite acesso RDP de entrada de endereços IP IPv4 na sua rede
Intervalo de endereços IPv6 da sua rede	TCP	3389	(Opcional) Permite acesso RDP de entrada de endereços IP IPv6 na sua rede

1. Criar a VPC

Use o procedimento a seguir para criar uma VPC com uma sub-rede pública em uma zona de disponibilidade. Esta configuração é adequada para um ambiente de desenvolvimento ou teste.

Como criar a VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel, escolha Criar VPC.
3. Em Resources to create (Recursos a serem criados), escolha VPC and more (VPC e mais).
4. Configurar a VPC
   a. Em Name tag auto-generation (Geração automática de tags de nome), insira um nome para a VPC.
   b. Em Bloco CIDR IPv4, é possível manter a sugestão padrão ou inserir o bloco CIDR exigido por sua aplicação ou rede. Para ter mais informações, consulte the section called “Blocos CIDR da VPC”.
   c. (Opcional) Se a sua aplicação se comunica usando endereços IPv6, escolha Bloco CIDR IPv6, Bloco CIDR IPv6 fornecido pela Amazon.
5. Configurar as sub-redes
   a. Em Número de zonas de disponibilidade, escolha 1. Você pode manter a zona de disponibilidade padrão ou expandir Personalizar AZs e selecionar uma zona de disponibilidade.
   b. Para Number of public subnets (Número de sub-redes públicas), escolha 1.
   c. Para Number of private subnets (Número de sub-redes privadas), escolha 0.
   d. É possível manter o bloco CIDR padrão para a sub-rede pública ou, alternativamente, expandir Personalizar blocos CIDR da sub-rede e inserir um bloco CIDR. Para ter mais informações, consulte the section called “Blocos CIDR de sub-redes”.
6. Em Gateways NAT, mantenha o valor padrão, Nenhum.
7. Em VPC endpoints (Endpoints de VPC), escolha None (Nenhum). Um endpoint da VPC de gateway para S3 é usado somente para acessar o Amazon S3 por meio de sub-redes privadas.
8. Em Opções de DNS, mantenha ambas as opções selecionadas. Como resultado, sua instância receberá um nome de host DNS público que corresponde a seu endereço IP público.
9. Escolha Criar VPC.

2. Implantar a aplicação

Há várias formas de implantar instâncias do EC2. Por exemplo:

- Assistente de inicialização de instâncias do Amazon EC2
- Amazon EC2 Auto Scaling
- AWS CloudFormation
- Amazon Elastic Container Service (Amazon ECS)

Após implantar uma instância do EC2, você poderá se conectar à instância, instalar o software necessário para a aplicação e, em seguida, criar uma imagem para uso futuro. Para obter mais informações, consulte Criar uma AMI no Guia do usuário do Amazon EC2. Como alternativa, é possível usar o EC2 Image Builder para criar e gerenciar sua Amazon Machine Image (AMI).

3. Testar a configuração

Após concluir a implantação da aplicação, você poderá testá-la. Se você não conseguir se conectar à instância do EC2 ou se a aplicação não conseguir enviar ou receber o tráfego esperado, você poderá usar o Reachability Analyzer para obter ajuda para solucionar problemas. Por exemplo, o Reachability Analyzer pode identificar problemas de configuração com suas tabelas de rotas ou grupos de segurança. Para obter mais informações, consulte o Guia do Analisador de Acessabilidade.

4. Limpeza

Quando essa configuração não for mais necessária, você poderá excluí-la. Antes de excluir a VPC, é necessário terminar a instância. Para ter mais informações, consulte the section called “Excluir a VPC:”.

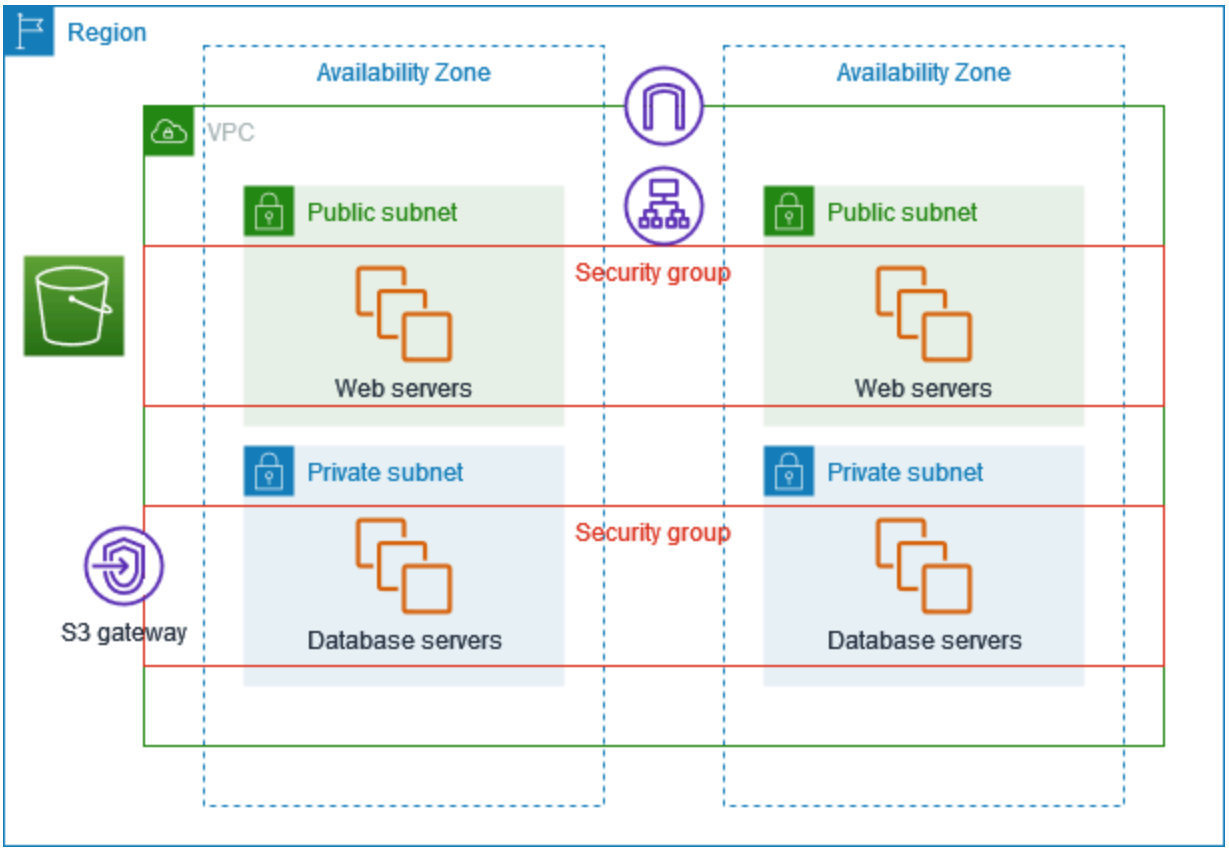
Exemplo: VPC para servidores Web e de banco de dados

Este exemplo demonstra como criar uma VPC que pode ser usada em uma arquitetura com dois níveis em um ambiente de produção. Para melhorar a resiliência, os servidores serão implantados em duas zonas de disponibilidade.

Conteúdo

Visão geral

O diagrama a seguir fornece uma visão geral dos recursos incluídos neste exemplo. A VPC tem sub-redes públicas e sub-redes privadas em duas zonas de disponibilidade. Os servidores Web são executados nas sub-redes públicas e recebem tráfego dos clientes por meio de um balanceador de carga. O grupo de segurança dos servidores Web permite tráfego do balanceador de carga. Os servidores de banco de dados são executados nas sub-redes privadas e recebem tráfego dos servidores Web. O grupo de segurança dos servidores de banco de dados permite tráfego dos servidores Web. Os servidores de banco de dados podem se conectar ao Amazon S3 usando um endpoint da VPC de gateway.



Roteamento

Quando essa VPC é criada usando a console da Amazon VPC, criamos uma tabela de rotas para as sub-redes públicas com rotas locais e rotas para o gateway da Internet e uma tabela de rotas para cada sub-rede privada com rotas locais e uma rota para o endpoint da VPC de gateway.

Veja a seguir um exemplo de tabela de rotas para sub-redes públicas com rotas para IPv4 e IPv6. Se você criar sub-redes somente IPv4 em vez de sub-redes de pilha dupla, sua tabela de rotas terá somente as rotas IPv4.

Destination (Destino)	Destino
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
0.0.0.0/0	*igw-id*
::/0	*igw-id*

Veja a seguir um exemplo de tabela de rotas para as sub-redes privadas com rotas locais para IPv4 e IPv6. Se você criou sub-redes somente IPv4, a tabela de rotas terá somente a rota IPv4. A última rota envia tráfego destinado ao Amazon S3 para o endpoint da VPC de gateway.

Destination (Destino)	Destino
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
s3-prefix-list-id	*s3-gateway-id*

Segurança

Para este exemplo de configuração, crie um grupo de segurança para o balanceador de carga, um grupo de segurança para os servidores Web e um grupo de segurança para os servidores de banco de dados.

Load balancer

O grupo de segurança do Application Load Balancer ou Network Load Balancer deve permitir tráfego de entrada de clientes na porta do receptor do balanceador de carga. Para aceitar tráfego de qualquer lugar na Internet, especifique 0.0.0.0/0 como origem. O grupo de segurança do balanceador de carga também deve permitir tráfego de saída do balanceador de carga para as instâncias de destino na porta do receptor da instância e na porta de verificação de integridade.

Servidores da web

As regras de grupos de segurança a seguir permitem que os servidores Web recebam tráfego HTTP e HTTPS do balanceador de carga. Opcionalmente, é possível permitir que os servidores Web recebam tráfego SSH ou RDP da sua rede. Os servidores Web podem enviar tráfego SQL ou MySQL para um servidor de banco de dados.

Origem	Protocolo	Intervalo de portas	Descrição
ID do grupo de segurança para o balanceador de carga	TCP	80	Permite acesso HTTP de entrada do balanceador de carga
ID do grupo de segurança para o balanceador de carga	TCP	443	Permite acesso HTTPS de entrada do balanceador de carga
Intervalo de endereços IPv4 públicos da sua rede	TCP	22	(Opcional) Permite acesso SSH de entrada de endereços IP IPv4 na sua rede
Intervalo de endereços IPv6 da sua rede	TCP	22	(Opcional) Permite acesso SSH de entrada de endereços IP IPv6 na sua rede

Origem	Protocolo	Intervalo de portas	Descrição
Intervalo de endereços IPv4 públicos da sua rede	TCP	3389	(Opcional) Permite acesso RDP de entrada de endereços IP IPv4 na sua rede
Intervalo de endereços IPv6 da sua rede	TCP	3389	(Opcional) Permite acesso RDP de entrada de endereços IP IPv6 na sua rede

Destination (Destino)	Protocolo	Intervalo de portas	Descrição
ID do grupo de segurança para instâncias que executam o Microsoft SQL Server	TCP	1433	Permite acesso de saída do Microsoft SQL Server aos servidores de banco de dados
ID do grupo de segurança para instâncias que executam MySQL	TCP	3306	Permite acesso de saída do MySQL aos servidores de banco de dados

Servidores de banco de dados

As regras de grupo de segurança a seguir permitem que os servidores de banco de dados recebam solicitações de leitura e gravação dos servidores Web.

Origem	Protocolo	Intervalo de portas	Comentários
ID do grupo de segurança do servidor Web	TCP	1433	Permite acesso de entrada ao Microsoft SQL Server proveniente dos servidores Web
ID do grupo de segurança do servidor Web	TCP	3306	Permite acesso de entrada ao MySQL Server proveniente dos servidores Web

Destination (Destino)	Protocolo	Intervalo de portas	Comentários
0.0.0.0/0	TCP	80	Permite acesso HTTP de saída à Internet via IPv4
0.0.0.0/0	TCP	443	Permite acesso HTTPS de saída à Internet via IPv4

Para obter mais informações sobre grupos de segurança para instâncias de banco de dados do RDS, consulte Controlar acesso com grupos de segurança no Manual do usuário do Amazon RDS.

1. Criar a VPC

Use o procedimento a seguir para criar uma VPC com uma sub-rede pública e uma sub-rede privada em duas zonas de disponibilidade.

Como criar a VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel, escolha Criar VPC.
3. Em Resources to create (Recursos a serem criados), escolha VPC and more (VPC e mais).
4. Configurar a VPC:

a. Mantenha a opção Geração automática de tags de nome selecionada para criar tags de nome para os recursos da VPC ou desmarque-a para fornecer suas próprias tags de nome para os recursos da VPC.

b. Em Bloco CIDR IPv4, é possível manter a sugestão padrão ou inserir o bloco CIDR exigido por sua aplicação ou rede. Para ter mais informações, consulte the section called “Blocos CIDR da VPC”.

c. (Opcional) Se a sua aplicação se comunica usando endereços IPv6, escolha Bloco CIDR IPv6, Bloco CIDR IPv6 fornecido pela Amazon.

d. Escolha uma opção de Locação. Essa opção define se as instâncias do EC2 que você executa na VPC serão executadas em hardware compartilhado com outras Contas da AWS ou em hardware dedicado somente para seu uso. Se você escolher que a locação da VPC seja `Default`, as instâncias do EC2 executadas nessa VPC usarão o atributo de locação especificado quando você executar a instância. Para obter mais informações, consulte Iniciar uma instância usando parâmetros definidos no Guia do usuário do Amazon EC2. Se você escolher a locação da VPC para ser `Dedicated`, as instâncias sempre serão executadas como Instâncias dedicadas no hardware dedicado ao seu uso.

5. Configurar as sub-redes:

a. Em Número de zonas de disponibilidade, escolha 2, para que você possa iniciar instâncias em duas zonas de disponibilidade para aumentar a resiliência.

b. Em Number of public subnets (Número de sub-redes públicas), escolha 2.

c. Em Number of private subnets (Número de sub-redes privadas), escolha 2.

d. É possível manter os blocos CIDR padrão para a sub-rede pública ou, alternativamente, expandir Personalizar blocos CIDR da sub-rede e inserir um bloco CIDR. Para ter mais informações, consulte the section called “Blocos CIDR de sub-redes”.

6. Em Gateways NAT, mantenha o valor padrão, Nenhum.

7. Para Endpoints da VPC, mantenha o valor padrão, Gateway do S3. Embora não haja efeito a menos que você acesse um bucket do S3, não há custo para habilitar esse endpoint da VPC.

8. Em Opções de DNS, mantenha ambas as opções selecionadas. Como resultado, seus servidores Web receberão nomes de host DNS públicos que correspondem aos seus endereços IP públicos.

9. Escolha Criar VPC.

2. Implantar o aplicativo

Idealmente, você já testou seus servidores Web e servidores de banco de dados em um ambiente de desenvolvimento ou teste e criou os scripts ou imagens que usará para implantar sua aplicação no ambiente de produção.

É possível usar instâncias do EC2 para seus servidores Web. Há várias formas de implantar instâncias do EC2. Por exemplo:

- Assistente de inicialização de instâncias do Amazon EC2
- AWS CloudFormation
- Amazon Elastic Container Service (Amazon ECS)

Para a aumentar a disponibilidade, é possível usar o Amazon EC2 Auto Scaling para implantar servidores em várias zonas de disponibilidade e manter a capacidade mínima de servidor exigida por sua aplicação.

O Elastic Load Balancing pode ser usado para distribuir tráfego uniformemente entre seus servidores. É possível anexar o balanceador de carga a um grupo do Auto Scaling.

Você pode usar instâncias do EC2 para seus servidores de banco de dados ou um de nossos tipos de banco de dados com propósito específico. Para obter mais informações, consulte Bancos de dados na AWS: como escolher.

3. Testar a configuração

Após concluir a implantação da aplicação, você poderá testá-la. Se a aplicação não conseguir enviar ou receber o tráfego esperado, você poderá usar o Reachability Analyzer para obter ajuda para solucionar problemas. Por exemplo, o Reachability Analyzer pode identificar problemas de configuração com suas tabelas de rotas ou grupos de segurança. Para obter mais informações, consulte o Guia do Analisador de Acessabilidade.

4. Limpeza

Quando essa configuração não for mais necessária, você poderá excluí-la. Antes de excluir a VPC, é necessário terminar as instâncias e excluir o balanceador de carga. Para ter mais informações, consulte the section called “Excluir a VPC:”.

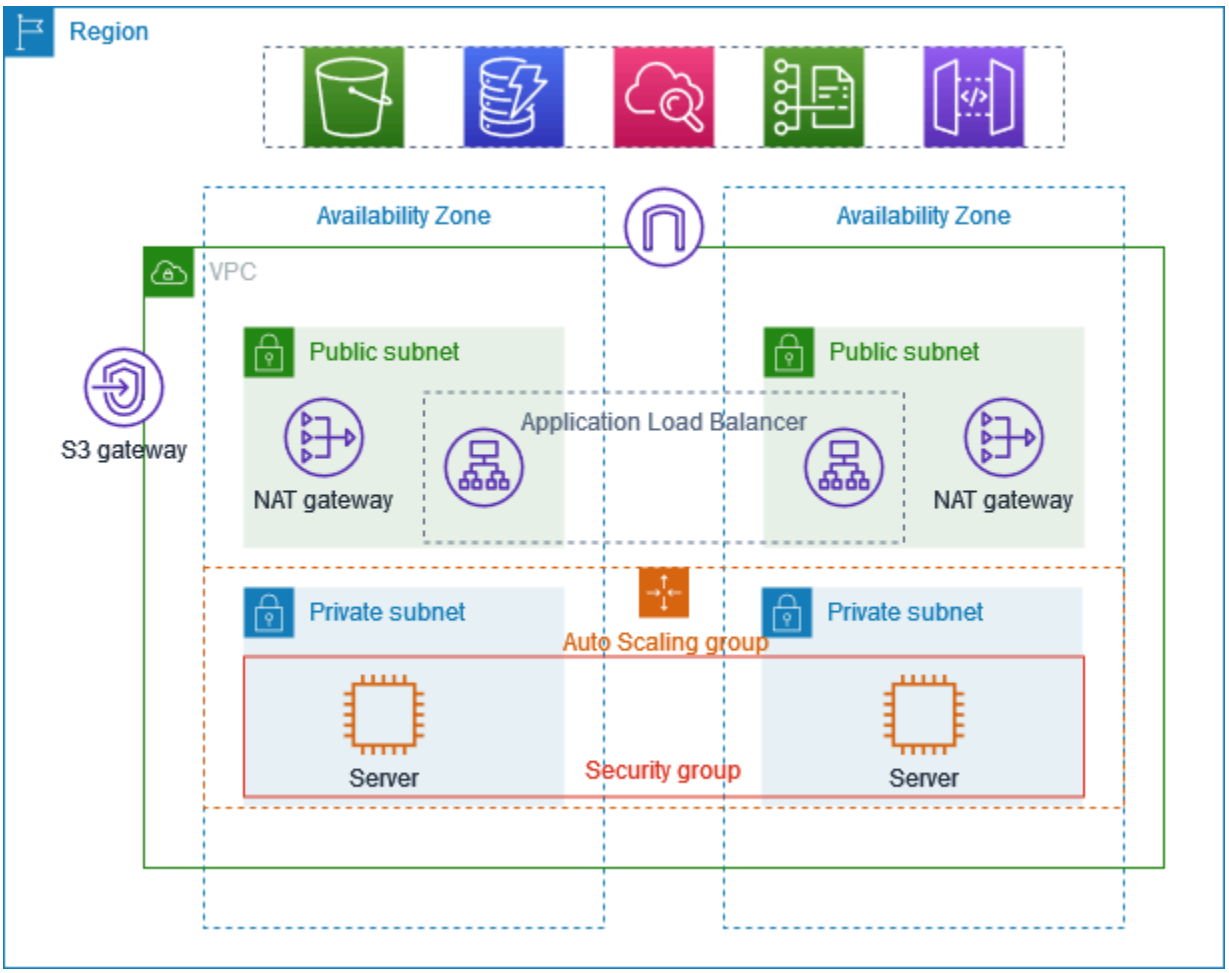
Exemplo: VPC com servidores em sub-redes privadas e NAT

Este exemplo demonstra como criar uma VPC que pode ser usada para servidores em um ambiente de produção. Para melhorar a resiliência, os servidores serão implantados em duas zonas de disponibilidade usando um grupo do Auto Scaling e um Application Load Balancer. Para maior segurança, os servidores serão implantados em sub-redes privadas. Os servidores recebem solicitações por meio do balanceador de carga. Os servidores podem se conectar à Internet usando um gateway NAT. Para melhorar a resiliência, o gateway NAT será implantado nas duas zonas de disponibilidade.

Conteúdo

Visão geral

O diagrama a seguir fornece uma visão geral dos recursos incluídos neste exemplo. A VPC tem sub-redes públicas e sub-redes privadas em duas zonas de disponibilidade. Cada sub-rede pública contém um gateway NAT e um nó balanceador de carga. Os servidores executados nas sub-redes privadas são executados e encerrados usando um grupo do Auto Scaling e recebem tráfego do balanceador de carga. Os servidores podem se conectar à Internet usando o gateway NAT. Os servidores podem se conectar ao Amazon S3 usando um endpoint da VPC de gateway.



Roteamento

Quando essa VPC é criada usando a console da Amazon VPC, criamos uma tabela de rotas para as sub-redes públicas com rotas locais e rotas para o gateway da Internet. Também criamos uma tabela de rotas para as sub-redes privadas com rotas locais e rotas para o gateway NAT, o gateway da Internet somente de saída e o endpoint da VPC de gateway.

Veja a seguir um exemplo da tabela de rotas para sub-redes públicas com rotas para IPv4 e IPv6. Se você criar sub-redes somente IPv4 em vez de sub-redes de pilha dupla, sua tabela de rotas incluirá somente as rotas IPv4.

Destination (Destino)	Destino
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local

Destination (Destino)	Destino
0.0.0.0/0	*igw-id*
::/0	*igw-id*

Veja a seguir um exemplo de tabela de rotas para uma das sub-redes privadas com rotas para IPv4 e IPv6. Se você criou sub-redes somente IPv4, a tabela de rotas incluirá somente as rotas IPv4. A última rota envia tráfego destinado ao Amazon S3 para o endpoint da VPC de gateway.

Destination (Destino)	Destino
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
0.0.0.0/0	*nat-gateway-id*
::/0	*eigw-id*
s3-prefix-list-id	*s3-gateway-id*

Segurança

Veja a seguir um exemplo das regras podem ser criadas para o grupo de segurança associado por você aos seus servidores. O grupo de segurança deve permitir o tráfego do balanceador de carga pela porta e pelo protocolo do receptor. Ele também deve permitir o tráfego de verificação de integridade.

Origem	Protocolo	Intervalo de portas	Comentários
ID do balanceador de carga do grupo de segurança	*protocolo do receptor*	*porta do receptor*	Permite tráfego de entrada do balanceador de carga na porta do receptor

Origem	Protocolo	Intervalo de portas	Comentários
ID do balanceador de carga do grupo de segurança	*protocolo de verificação de integridade*	*porta de verificação de integridade*	Permite tráfego de entrada da verificação de integridade proveniente do balanceador de carga

1. Criar a VPC

Use o procedimento a seguir para criar uma VPC com uma sub-rede pública e uma sub-rede privada em duas zonas de disponibilidade e um gateway NAT em cada zona de disponibilidade.

Como criar a VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel, escolha Criar VPC.
3. Em Resources to create (Recursos a serem criados), escolha VPC and more (VPC e mais).
4. Configurar a VPC
    a. Em Name tag auto-generation (Geração automática de tags de nome), insira um nome para a VPC.
    b. Em Bloco CIDR IPv4, é possível manter a sugestão padrão ou inserir o bloco CIDR exigido por sua aplicação ou rede.
    c. Se a sua aplicação se comunica usando endereços IPv6, escolha Bloco CIDR IPv6, Bloco CIDR IPv6 fornecido pela Amazon.
5. Configurar as sub-redes
    a. Em Número de zonas de disponibilidade, escolha 2, para que você possa iniciar instâncias em várias zonas de disponibilidade para aumentar a resiliência.
    b. Em Number of public subnets (Número de sub-redes públicas), escolha 2.
    c. Em Number of private subnets (Número de sub-redes privadas), escolha 2.

d. É possível manter o bloco CIDR padrão para a sub-rede pública ou, alternativamente, expandir Personalizar blocos CIDR da sub-rede e inserir um bloco CIDR. Para ter mais informações, consulte the section called “Blocos CIDR de sub-redes”.

6. Em Gateways NAT, escolha 1 por zona de disponibilidade para melhorar a resiliência.
7. Se a sua aplicação se comunica usando endereços IPv6, em Gateway da Internet somente de saída, escolha Sim.
8. Em Endpoints da VPC, caso suas instâncias precisem acessar um bucket do S3, mantenha o Gateway do S3 padrão. Caso contrário, as instâncias em sua sub-rede privada não poderão acessar o Amazon S3. Essa opção não tem custo, portanto, você poderá manter o padrão se quiser usar um bucket do S3 no futuro. Se você escolher Nenhum, sempre poderá adicionar um endpoint da VPC de gateway posteriormente.
9. Em Opções de DNS, desmarque Habilitar nomes de host de DNS.
10. Escolha Criar VPC.

2. Implantar o aplicativo

Idealmente, você terminou de testar seus servidores em um ambiente de desenvolvimento ou teste e criou os scripts ou imagens que usará para implantar sua aplicação no ambiente de produção.

É possível usar o Amazon EC2 Auto Scaling para implantar servidores em várias zonas de disponibilidade e manter a capacidade mínima de servidor exigida pela aplicação.

Para executar instâncias usando um grupo do Auto Scaling

1. Crie um modelo de execução para especificar as informações de configuração necessárias para executar suas instâncias do EC2 usando o Amazon EC2 Auto Scaling. Para obter instruções detalhadas, consulte Criar um modelo de inicialização para um grupo do Auto Scaling no Guia do usuário do Amazon EC2 Auto Scaling.
2. Crie um grupo do Auto Scaling, que é uma coleção de instâncias do EC2 com os tamanhos mínimo, máximo e desejado. Para obter instruções detalhadas, consulte Criar um grupo do Auto Scaling usando um modelo de inicialização no Guia do usuário do Amazon EC2 Auto Scaling.
3. Crie um balanceador de carga que distribua tráfego uniformemente entre as instâncias do grupo do Auto Scaling e anexe o balanceador de carga ao grupo do Auto Scaling. Para obter mais informações, consulte o Guia do usuário do Elastic Load Balancing e Usar o Elastic Load Balancing no Guia do usuário do Amazon EC2 Auto Scaling.

3. Testar a configuração

Após concluir a implantação da aplicação, você poderá testá-la. Se a aplicação não conseguir enviar ou receber o tráfego esperado, você poderá usar o Reachability Analyzer para obter ajuda para solucionar problemas. Por exemplo, o Reachability Analyzer pode identificar problemas de configuração com suas tabelas de rotas ou grupos de segurança. Para obter mais informações, consulte o Guia do Analisador de Acessabilidade.

4. Limpeza

Quando essa configuração não for mais necessária, você poderá excluí-la. Antes de excluir a VPC, é necessário excluir o grupo do Auto Scaling, encerrar suas instâncias, excluir os gateways NAT e excluir o balanceador de carga. Para ter mais informações, consulte the section called “Excluir a VPC:”.

Cotas da Amazon VPC

As tabelas a seguir listam as cotas, anteriormente denominadas limites, para os recursos da Amazon VPC para sua conta da AWS. Salvo indicado de outra forma, as cotas são por região.

Se solicitar um aumento de cota que seja aplicável por recurso, aumentaremos a cota para todos os recursos na Região.

VPC e sub-redes

Name	Padrão	Ajustável	Comentários
VPCs por Região	5	Sim	Se essa cota for aumentada, a cota em gateways da Internet por Região será aumentada no mesmo valor. É possível aumentar esse limite para ter centenas de VPCs por região.
Sub-redes por VPC	200	Sim	
Blocos CIDR IPv4 por VPC	5	Sim (até 50)	Esse bloco CIDR primário e todos os blocos CIDR secundários são contabilizados de acordo com essa cota.
Blocos CIDR IPv6 por VPC	5	Sim (até 50)	O número de CIDRs que é possível alocar para uma única VPC.
Exclusões do Bloquear o Acesso Público da VPC por conta, por região	50	Sim. Para solicitar um aumento, abra um caso de aumento de limite de serviço usando	O número de exclusões do BPA da VPC que você pode criar em uma conta.

Name	Padrão	Ajustável	Comentários
		o AWS Support Center Console.	

DNS

Cada instância do EC2 pode enviar 1024 pacotes por segundo por interface de rede para o Route 53 Resolver (especificamente o endereço .2, como 10.0.0.2 e 169.254.169.253). Essa cota não pode ser aumentada. O número de consultas de DNS por segundo com suporte do Amazon Route 53 varia, dependendo do tipo da consulta, do tamanho da resposta e do protocolo em uso. Para obter mais informações e recomendações para uma arquitetura de DNS escalável, consulte o Guia técnico DNS híbrido da AWS com Diretório Ativo.

Endereços IP elásticos

Name	Padrão	Ajustável	Comentários
Endereços IP elásticos por Região	5	Sim	Essa cota se aplica a VPCs de Conta da AWS individuais e a VPCs compartil hadas.
Endereços IP elásticos por gateway de NAT público	2	Sim	É possível solicitar um aumento da cota até 8.

Gateways

Name	Padrão	Ajustável	Comentários
Gateways da Internet somente de saída por Região	5	Sim	Para aumentar essa cota, aumente a cota para VPCs por região. Só é possível anexar um gateway da Internet somente de saída a uma VPC de cada vez.

Name	Padrão	Ajustável	Comentários
Gateways da Internet por Região	5	Sim	Para aumentar essa cota, aumente a cota para VPCs por região. Só é possível anexar um gateway da Internet a uma VPC de cada vez.
Gateways de NAT por zona de disponibilidade	5	Sim	Os gateways NAT só são contabilizados em sua cota nos estados `pending`, `active` e `deleting`.
Cota de endereço IP privado por gateway NAT	8	Sim	
Gateways de operadora por VPC	1	Não	

Listas de prefixos gerenciadas pelo cliente

Embora as cotas padrão para listas de prefixos gerenciadas pelo cliente sejam ajustáveis, não é possível ajustar as cotas via console do Service Quotas. Para isso, é necessário abrir um caso de aumento do limite de serviço via AWS Support Center Console.

Name	Padrão	Ajustável	Comentários
Listas de prefixos por Região	100	Sim	
Versões por lista de prefixos	1.000	Sim	Se uma lista de prefixos tem mil versões armazenadas e você adiciona uma nova, a versão mais antiga é removida para permitir que a nova seja adicionada.
Número máximo de entradas por lista de prefixos	1.000	Sim	Você pode redimensionar uma lista de prefixos gerenciada pelo cliente em até 1000. Para ter mais informações, consulte Redimensionar uma lista de

Name	Padrão	Ajustável	Comentários
			prefixos. Quando você faz referência a uma lista de prefixos em um recurso, o número máximo de entradas para as listas de prefixos é considerado como parte da cota para o número de entradas para o recurso. Por exemplo, se você cria uma lista de prefixos com o máximo de 20 entradas e faz referência a essa lista de prefixos em uma regra do grupo de segurança, isso contará como 20 regras para o grupo de segurança.
Referências a uma lista de prefixos por tipo de recurso	5.000	Sim	Essa cota se aplica de acordo com o tipo de recurso que pode fazer referênci a a uma lista de prefixos. Por exemplo, você pode ter 5 mil referências a uma lista de prefixos em todos os grupos de segurança mais 5 mil referências a uma lista de prefixos em todas as tabelas de rotas da sub-rede. Se você compartilhar uma lista de prefixos com outras contas da AWS, as referências das outras contas à sua lista de prefixos serão contabilizadas nessa cota.

Network ACLs

Name	Padrão	Ajustável	Comentários
ACLs de rede por VPC	200	Sim	É possível associar uma ACL de rede a uma ou mais sub-redes em uma VPC.
Regras por ACL de rede	20	Sim	Essa cota determina o número máximo de regras de entrada e de saída. Ela

Name	Padrão	Ajustável	Comentários
			pode ser aumentada até no máximo 40 regras de entrada e 40 regras de saída (totalizando 80 regras), mas o desempenho da rede pode ser afetado.

Interfaces de rede

Name	Padrão	Ajustável	Comentários
Interfaces de rede por instância	Varia por tipo de instância	Não	Para obter mais informações, consulte Interfaces de rede por tipo de instância.
Interfaces de rede por Região	5.000	Sim	Essa cota se aplica a VPCs de Conta da AWS individuais e a VPCs compartilhadas. Esse limite é aplicado por zona de disponibilidade (AZ). Por exemplo, se as interfaces de rede estiverem em 3 AZs, cada AZ terá um limite de 5.000 e a região terá um limite de 15.000.

Tabelas de rotas

Name	Padrão	Ajustável	Comentários
Tabelas de rotas por VPC	200	Sim	A tabela de rotas principal é contabilizada de acordo com essa cota. Observe que, se você solicitar um aumento de cota para tabelas de rotas, talvez também queira solicitar um aumento de cota para sub-redes. Enquanto tabelas de rota podem ser compartilhadas com

Name	Padrão	Ajustável	Comentários
			várias sub-redes, uma sub-rede pode ser associada a apenas uma tabela de rotas.
Rotas por tabela de rotas (rotas não propagadas)	50	Sim	Você pode aumentar essa cota até 1.000. No entanto, isso pode afetar o performance da rede. Essa cota é imposta separadamente para rotas IPv4 e IPv6. Se você tiver mais de 125 rotas, é recomendável paginar chamadas para descrever suas tabelas de rotas para melhor performance.
Rotas propagadas por tabela de rotas	100	Não	Se você precisar de mais prefixos, anuncie uma rota padrão.

Grupos de segurança

Name	Padrão	Ajustável	Comentários
Grupos de segurança da VPC por Região	2.500	Sim	Essa cota se aplica a VPCs de Conta da AWS individuais e a VPCs compartil hadas. Se você aumentar essa cota para mais de 5 mil grupos de segurança em uma Região, recomendamos paginar as chamadas para descrever seus grupos de segurança e obter melhor performan ce.
As regras de entrada ou de saída por grupo de segurança	60	Sim	Essa limitação é aplicada de forma independente para regras de entrada e de saída. Para uma conta com a

Name	Padrão	Ajustável	Comentários
			cota padrão de 60 regras, um grupo de segurança pode ter até 60 regras de entrada e 60 regras de saída. Além disso, essa limitação é aplicada separadamente para regras IPv4 e regras IPv6. Para uma conta com a cota padrão de 60 regras, um grupo de segurança pode ter até 60 regras de entrada para tráfego IPv4 e 60 regras de entrada para tráfego IPv6. Para ter mais informações, consulte the section called "Tamanho do grupo de segurança". Uma alteração de cota é aplicada às regras de entrada e saída. Essa cota multiplicada pela cota para os grupos de segurança por interface de rede não pode exceder 1000.
Grupos de segurança por interface de rede	5	Sim (até 16)	Essa cota multiplicada pela cota das regras por grupo de segurança não pode exceder 1.000.

compartilhamento sub-rede VPC

Todas as cotas padrão da VPC são aplicáveis a sub-redes compartilhadas da VPC.

Name	Padrão	Ajustável	Comentários
Contas participantes por VPC	100	Sim	O número de contas de participantes distintas com as quais as sub-redes de uma VPC podem ser compartilhadas. Essa é uma cota por VPC, que se aplica a todas as sub-redes compartilhadas em uma VPC.

Name	Padrão	Ajustável	Comentários
			Os proprietários da VPC podem visualizar as interfaces de rede e os grupos de segurança anexados aos recursos do participante.
As sub-redes que podem ser compartilhadas com uma conta	100	Sim	Esse é o número máximo de sub-redes que podem ser compartilhadas com uma conta da AWS.

Uso de endereço de rede

O uso de endereço de rede (NAU) é composto de endereços IP, interfaces de rede e CIDRs em listas de prefixos gerenciados. O (NAU) é uma métrica aplicada aos recursos em uma VPC para ajudar você a planejar e monitorar o tamanho da sua VPC. Para ter mais informações, consulte Uso de endereço de rede.

Os recursos que compõem a contagem de NAU têm suas próprias service quotas individuais. Mesmo que uma VPC tenha capacidade de NAU disponível, você não poderá lançar recursos na VPC se os recursos tiverem excedido suas service quotas.

Name	Padrão	Ajustável	Comentários
Uso de endereço de rede	64.000	Sim (até 256.000)	O número máximo de unidades de NAU por VPC.
Uso de endereços de rede emparelhados	128.000	Sim (até 512.000)	O número máximo de unidades de NAU para uma VPC e todas as suas VPCs emparelhadas na mesma região. VPCs que estão emparelhadas em regiões diferentes não contribuem para esse número.

Controle de utilização da API do Amazon EC2

Para obter informações sobre o controle de utilização do Amazon EC2, consulte Request throttling no Guia do desenvolvedor do Amazon EC2.

Recursos de cota adicionais

Para obter mais informações, consulte:

- Cotas do AWS Client VPN no Guia do administrador do AWS Client VPN
- Cotas do AWS Direct Connect no Manual do usuário do AWS Direct Connect
- Emparelhamento de cotas no Guia de emparelhamento da Amazon VPC
- Cotas do PrivateLink no Guia de AWS PrivateLink
- Cotas do Site-to-Site VPN no Manual do usuário do AWS Site-to-Site VPN
- Cotas de espelhamento de tráfego no Guia do Amazon VPC Traffic Mirroring
- Cotas do Transit Gateway no Guia do Amazon VPC Transit Gateways

Histórico do documento

A tabela a seguir descreve as alterações importantes em cada versão do Guia do usuário da Amazon VPC.

Alteração	Descrição	Data
Atualização da política gerenciada da AWS	A Amazon VPC atualizou as políticas gerenciadas AmazonVPCFullAccess e AmazonVPCReadOnlyAccess.	9 de dezembro de 2024
Suporte para políticas declarativas para o BPA na VPC	Caso esteja usando o AWS Organizations para gerenciar as contas da sua organização, é possível usar uma política declarativa para aplicar o BPA da VPC nas contas da organização.	1.º de dezembro de 2024
Bloquear o Acesso Público (BPA) da VPC	O atributo Bloquear o Acesso Público (BPA) da VPC permite impedir que os recursos nas VPCs e sub-redes que você possui em uma região acessem ou sejam acessados pela Internet por meio de gateways da Internet e gateways da Internet somente de saída.	19 de novembro de 2024
Grupos de Segurança Compartilhados	Esse atributo permite que você compartilhe um grupo de segurança com outras contas do AWS Organizations.	30 de outubro de 2024

Associações de Grupos de Segurança a VPCs	Esse atributo permite associar um grupo de segurança a várias VPCs na mesma região.	30 de outubro de 2024
Suporte à MTU do gateway NAT	Os gateways NAT oferecem suporte a tráfego com uma unidade de transmissão máxima (MTU) de 8500.	10 de setembro de 2024
Endereçamento IPv6 privado	Foram adicionadas informaçõ es sobre endereçamento IPv6 privado. Os endereços IPv6 privados só estão disponíveis no Gerenciador de endereços IP da Amazon VPC.	8 de agosto de 2024
Tempo de locação preferencial de IPv6	Agora você pode escolher com que frequência uma instância em execução com um IPv6 atribuído a ela passa pela renovação do leasing DHCPv6.	20 de fevereiro de 2024
Revisão e melhorias na estrutura do guia	A estrutura do guia foi revisada e melhorias foram feitas para melhorar a experiência do cliente em relação à busca de informaçõ es para cenários específicos.	20 de fevereiro de 2024
Atualização da política gerenciada da AWS	A Amazon VPC atualizou as políticas gerenciadas AmazonVPCFullAccess e AmazonVPCReadOnlyAccess.	8 de fevereiro de 2024

Atualização da política gerenciada da AWS	A Amazon VPC atualizou a política gerenciada AmazonVPCCrossAccountNetworkInterfaceOperations.	25 de setembro de 2023
O EC2-Classic foi descontinuado	Com o EC2-Classic, suas instâncias do EC2 executadas em uma única rede simples compartilhada com outros clientes. A Amazon VPC substitui o EC2-Classic. Com a Amazon VPC, suas instâncias são executadas em uma nuvem privada virtual (VPC) que é isolada logicamente na Conta da AWS.	31 de julho de 2023
Adicionar endereços IPv4 secundários a gateways NAT	Você pode adicionar endereços IPv4 privados secundários a gateways NAT públicos e privados. Os endereços IPv4 secundários aumentam o número de portas disponíveis e, portanto, aumentam o limite do número de conexões simultâneas que suas workloads podem estabelecer usando um gateway NAT.	31 de janeiro de 2023
Como se alinhar com as práticas recomendadas do IAM	Guia atualizado para alinhamento com as práticas recomendadas do IAM. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM.	4 de janeiro de 2023

Escolher o endereço IP privado do seu gateway NAT	Agora, ao criar um gateway NAT, é possível escolher o endereço IP privado atribuído ao gateway NAT. Anteriorm ente, o endereço IP privado do intervalo de endereços IP da sub-rede.	17 de novembro de 2022
Configuração de roteador de gateway padrão IPv6	Agora, três endereços IPv6 estão reservados para uso pelo roteador da VPC padrão.	11 de novembro de 2022
Transferir endereços IP elásticos	Agora você pode transferir endereços IP elásticos de uma conta da AWS para outra.	31 de outubro de 2022
Métricas de uso de endereço de rede	Você pode ativar as métricas de uso de endereço de rede para sua VPC para ajudar no planejamento e no monitoram ento do tamanho da sua VPC.	04 de outubro de 2022
Publicar logs de fluxo no Amazon Data Firehose	Você pode especificar um fluxo de entrega do Amazon Data Firehose como um destino para os dados do log de fluxo.	8 de setembro de 2022
Largura de banda do gateway NAT	Gateways NAT agora oferecem suporte a larguras de banda de até 100 Gbps (um aumento de 45 Gbps) e são capazes de processar até dez milhões de pacotes por segundo (um aumento de quatro milhões de pacotes).	15 de junho de 2022

Diversos blocos CIDR IPv6	Você pode associar até cinco blocos CIDR IPv6 a uma VPC.	12 de maio de 2022
Reorganização	Reorganização geral deste Guia do usuário da Amazon Virtual Private Cloud.	2 de janeiro de 2022
Gateway NAT IPv6 para IPv4	O gateway NAT oferece suporte à conversão de endereços de rede de IPv6 para IPv4, mais conhecida como NAT64.	24 de novembro de 2021
Sub-redes somente IPv6 em VPCs	Você pode criar sub-redes somente IPv6 em que poderá iniciar instâncias do EC2 somente IPv6.	23 de novembro de 2021
Opções de entrega do VPC Flow Logs para o Amazon S3	Você pode especificar o formato de arquivo de log do Apache Parquet, partições por hora e prefixos S3 compatíveis com o Hive.	13 de outubro de 2021
Amazon EC2 Global View	O Amazon EC2 Global View permite que você visualize VPCs, sub-redes, instância s, grupos de segurança e volumes em várias regiões do AWS em um único console.	1º de setembro de 2021

Rotas mais específicas	Você pode adicionar uma rota às suas tabelas de rotas que seja mais específica do que a rota local. Você pode usar rotas mais específicas para redirecionar tráfego entre sub-redes em uma VPC (tráfego leste-oeste) para um dispositivo middlebox. Você pode definir o destino de uma rota para corresponder a todo o bloco CIDR IPv4 ou IPv6 de uma sub-rede em sua VPC.	30 de agosto de 2021
IDs de recursos e suporte a marcação para regras do grupo de segurança	É possível fazer referência a regras de grupo de segurança por ID de recurso. Também é possível adicionar tags a regras de grupos de segurança.	7 de julho de 2021
Gateways NAT privados	Você pode usar um gateway NAT privado para estabelecer comunicação privada somente de saída entre VPCs ou entre uma VPC e sua rede on-premises.	10 de junho de 2021
Tag na criação	É possível adicionar tags ao criar uma VPC, opções de DHCP, gateway da Internet, gateway somente de saída, network ACL e grupo de segurança.	30 de junho de 2020

Listas de prefixos gerenciados	Você pode criar e gerenciar um conjunto de blocos CIDR na lista de prefixos.	29 de junho de 2020
Melhorias de logs de fluxo	Novos campos de log de fluxo estão disponíveis e é possível especificar um formato personalizado para logs de fluxo que publicam no CloudWatch Logs.	4 de maio de 2020
Suporte à marcação para logs de fluxo	É possível adicionar tags aos logs de fluxo.	16 de março de 2020
Tag na criação do gateway NAT	É possível adicionar uma tag ao criar um gateway NAT.	9 de março de 2020
Intervalo de agregação máximo para logs de fluxo	É possível especificar o período máximo durante o qual um fluxo é capturado e agregado em um registro de log de fluxo.	4 de fevereiro de 2020
Configuração do grupo de borda de rede	É possível configurar grupos de borda de rede para suas VPCs no Amazon Virtual Private Cloud Console.	22 de janeiro de 2020
Tabelas de rotas do gateway	É possível associar uma tabela de rotas a um gateway e rotear o tráfego de entrada da VPC para uma interface de rede específica na VPC.	3 de dezembro de 2019

Melhorias de logs de fluxo	É possível especificar um formato personalizado para o log de fluxo e escolher quais campos retornar nos registros de log de fluxo.	11 de setembro de 2019
Compartilhamento VPC	Você pode compartilhar sub-redes que estão na mesma VPC com várias contas na mesma organização da AWS.	27 de novembro de 2018
Criar sub-rede padrão	Você pode criar uma sub-rede padrão em uma zona de disponibilidade que não tenha uma.	9 de novembro de 2017
Suporte à marcação para gateways NAT	Você pode marcar o gateway NAT.	7 de setembro de 2017
Métricas do Amazon CloudWatch para gateways NAT	É possível visualizar métricas do CloudWatch para o gateway NAT.	7 de setembro de 2017
Descrições de regras do security group	Você pode adicionar descrições às regras do security group.	31 de agosto de 2017
Blocos CIDR IPv4 secundários para a VPC	Você pode adicionar vários blocos CIDR IPv4 à VPC.	29 de agosto de 2017
Recuperar endereços IP elásticos	Se liberar um endereço IP elástico, você poderá recuperá-lo.	11 de agosto de 2017
Criar a VPC padrão	É possível criar uma nova VPC padrão se você excluir a VPC padrão existente.	27 de julho de 2017

Suporte a IPv6	Você pode associar um bloco CIDR IPv6 à sua VPC e atribuir endereços IPv6 a recursos em sua VPC.	1 de dezembro de 2016
Suporte de resolução de DNS para intervalos de endereços IP fora da RFC 1918	O servidor de DNS da Amazon agora pode determinar nomes de host DNS privados para endereços IP privados, para todos os espaços de endereço.	24 de outubro de 2016
Gateways NAT	É possível criar um gateway NAT em uma sub-rede pública e permitir que instâncias em uma sub-rede privada iniciem tráfego de saída para a Internet ou outros serviços da AWS.	17 de dezembro de 2015
VPC Flow Logs	Você pode criar um log de fluxo para capturar informaçõ es sobre o tráfego de IP para e proveniente das interfaces de rede em sua VPC.	10 de junho de 2015
ClassicLink	É possível usar o ClassicLink para vincular sua instância do EC2-Classic a uma VPC em sua conta. É possível associar grupos de segurança da VPC à instância do EC2-Classic habilitando a comunicação entre sua instância do EC2-Classic e as instâncias em sua VPC usando endereços IP privados.	7 de janeiro de 2015

Uso de zonas hospedadas privadas	É possível acessar recursos em sua VPC usando nomes de domínio de DNS personalizados que podem ser definidos em uma zona hospedada privada no Route 53.	5 de novembro de 2014
Modificação de um atributo de endereçamento IP público	Você pode modificar o atributo de endereçamento IP público de sua sub-rede para indicar se as instâncias executadas nessa sub-rede devem receber endereço IP público.	21 de junho de 2014
Atribuição de um endereço IP público	É possível atribuir um endereço IP público a uma instância durante a inicialização.	20 de agosto de 2013
Habilitação de nomes de host DNS e desabilitação de resolução de DNS	É possível modificar os padrões da VPC, desabilitar a resolução DNS e habilitar nomes de host DNS.	11 de março de 2013
VPC em todo o lugar	Adicionado de suporte a VPC em cinco regiões da AWS, VPCs em várias zonas de disponibilidade, várias VPCs por conta da AWS e várias conexões VPN por VPC.	3 de agosto de 2011
Instâncias dedicadas	Instâncias dedicadas são instâncias do Amazon EC2 executadas da sua VPC que executam o hardware dedicado a um único cliente.	27 de março de 2011