Amazon Virtual Private Cloud

Guia do usuário

Amazon Virtual Private Cloud: Guia do usuário

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e o visual comercial da Amazon não podem ser usados em conexão com nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa causar confusão entre os clientes ou que deprecie ou desacredite a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que é Amazon VPC?

A Amazon Virtual Private Cloud (Amazon VPC) permite executar recursos da AWS em uma rede virtual definida por você. Essa rede virtual se assemelha a uma rede tradicional que você operaria no seu datacenter, com os benefícios de usar a infraestrutura dimensionável da AWS.

Conceitos da Amazon VPC

A Amazon VPC é a camada de rede do Amazon EC2. Se você não tem experiência com o Amazon EC2, consulte O que é o Amazon EC2? no Guia do usuário do Amazon EC2 para instâncias do Linux para obter uma breve visão geral.

Veja a seguir os principais conceitos das VPCs:

- Virtual Private Cloud (VPC): uma rede virtual dedicada à sua conta da AWS.
- Sub-rede: um intervalo de endereços IP na VPC.
- Tabela de rotas: um conjunto de regras, chamadas de rotas, que são usadas para determinar para onde o tráfego de rede será direcionado.
- Gateway da Internet: um gateway que você anexa à VPC para permitir a comunicação entre recursos na VPC e a Internet.
- VPC endpoint: permite que você conecte de forma privada a VPC aos serviços da AWS compatíveis e aos serviços do VPC endpoint desenvolvidos pelo PrivateLink sem exigir um gateway da Internet, um dispositivo NAT, uma conexão VPN ou uma conexão do AWS Direct Connect. As instâncias na sua VPC não exigem que endereços IP públicos se comuniquem com recursos no serviço. O tráfego entre a sua VPC e os outros serviços não deixa a rede da Amazon. Para obter mais informações, consulte AWS PrivateLink e VPC endpoints (p. 343).
- Bloco CIDR: roteamento sem classe entre domínios. Uma metodologia de alocação de endereço de protocolo de Internet e agregação de rota. Para obter mais informações, consulte Roteamento sem classe entre domínios na Wikipédia.

Acessar a Amazon VPC

É possível criar, acessar e gerenciar as VPCs usando qualquer uma das seguintes interfaces:

- Console de Gerenciamento da AWS: fornece uma interface da Web que pode ser usada para acessar as VPCs.
- Interface da Linha de Comando da AWS (CLI da AWS): fornece comandos para um amplo conjunto de serviços da AWS, inclusive Amazon VPC, e é compatível com Windows, Mac e Linux. Para obter mais informações, consulte Interface da Linha de Comando da AWS.
- AWS SDKs: fornecem APIs específicas da linguagem 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 SDKs da AWS.
- API de consulta: fornece ações de API de baixo nível que são chamadas usando solicitações HTTPS. Usar a API de consulta é a maneira mais direta para acessar a Amazon VPC, mas exige que a aplicação lide com detalhes de baixo nível, como geração de hash para assinar a solicitação e tratamento de erros. Para obter mais informações, consulte a Referência de API do Amazon EC2.

Definição de preços da Amazon VPC

Não há custo adicional por usar a VPC. Há cobranças para os seguintes componentes da VPC: conexão do Site-to-Site VPN, PrivateLink, espelhamento de tráfego e gateway NAT. Para obter mais informações, consulte Definição de preço da Amazon VPC.

Cotas da Amazon VPC

Existem cotas para o número de componentes da Amazon VPC que você pode provisionar. É possível solicitar o aumento de algumas dessas cotas. Para obter mais informações, consulte Cotas da Amazon VPC (p. 345).

Conformidade do PCI DSS

A Amazon VPC é compatível com o processamento, o armazenamento e a transmissão de dados de cartão de crédito por um comerciante ou um provedor de serviços e foi validada como em conformidade com o Data Security Standard (DSS, Padrão de segurança de dados) da Payment Card Industry (PCI, Padrão de cartão de crédito). Para obter mais informações sobre PCI DSS, incluindo como solicitar uma cópia do pacote de conformidade com PCI da AWS, consulte Nível 1 do PCI DSS.

Como funciona a Amazon VPC

A Amazon Virtual Private Cloud (Amazon VPC) permite executar recursos da AWS em uma rede virtual definida por você. Essa rede virtual se assemelha a uma rede tradicional que você operaria no seu datacenter, com os benefícios de usar a infraestrutura dimensionável da AWS.

A Amazon VPC é a camada de rede do Amazon EC2. Se você não tem experiência com o Amazon EC2, consulte O que é o Amazon EC2? no Guia do usuário do Amazon EC2 para instâncias do Linux para obter uma breve visão geral.

Tópicos

VPCs e sub-redes

Uma virtual private cloud (VPC) é uma rede virtual dedicada à sua conta da AWS Ela é isolada de maneira lógica das outras redes virtuais na Nuvem AWS. Você pode executar os recursos da AWS, como instâncias do Amazon EC2, na VPC. Você pode especificar um intervalo de endereços IP para a VPC, adicionar sub-rede, associar security groups e configurar tabelas de rota.

Uma sub-rede é uma gama de endereços IP na VPC. Você pode executar recursos da AWS em uma sub-rede especificada. Use uma sub-rede pública para recursos que devem estar conectados à Internet e uma sub-rede privada para recursos que não estarão conectados à Internet.

Para proteger os recursos AWS em cada sub-rede, use várias camadas de segurança, incluindo grupos de segurança e Access Control Lists (ACL - listas de controle de acesso) de rede.

Associe, opcionalmente, um bloco CIDR IPv6 à VPC e atribua endereços IPv6 às instâncias em sua VPC.

Mais informações

- Conceitos básicos de sub-rede e VPC (p. 100)
- Privacidade do tráfego entre redes na Amazon VPC (p. 158)
- Endereçamento IP na sua VPC (p. 117)

VPCs padrão e não padrão

Se sua conta tiver sido criada depois de 4/12/2013, ela tem uma VPC padrão com uma sub-rede padrão em cada zona de disponibilidade. Uma VPC padrão detém os benefícios dos recursos avançados

fornecidos pelo EC2-VPC e está pronta para o uso. Caso você tenha um padrão VPC e não especifique uma sub-rede ao executar uma instância, a instância será iniciada no padrão VPC. É possível executar instâncias em sua VPC padrão sem precisar conhecer absolutamente nada sobre o Amazon VPC.

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.

Mais informações

- VPC e sub-redes padrão (p. 149)
- Conceitos básicos da Amazon VPC (p. 11)

Tabelas de rotas

Uma tabela de rotas contém um conjunto de regras chamado de rotas, que 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).

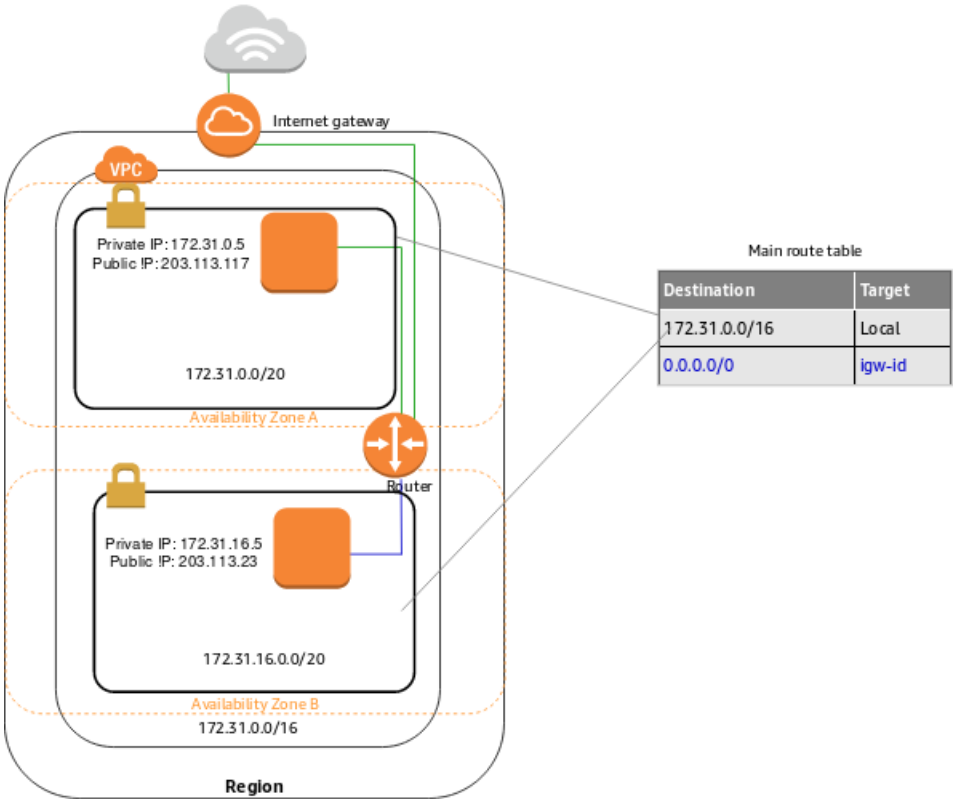
Mais informações

- Tabelas de rotas para sua VPC (p. 283)

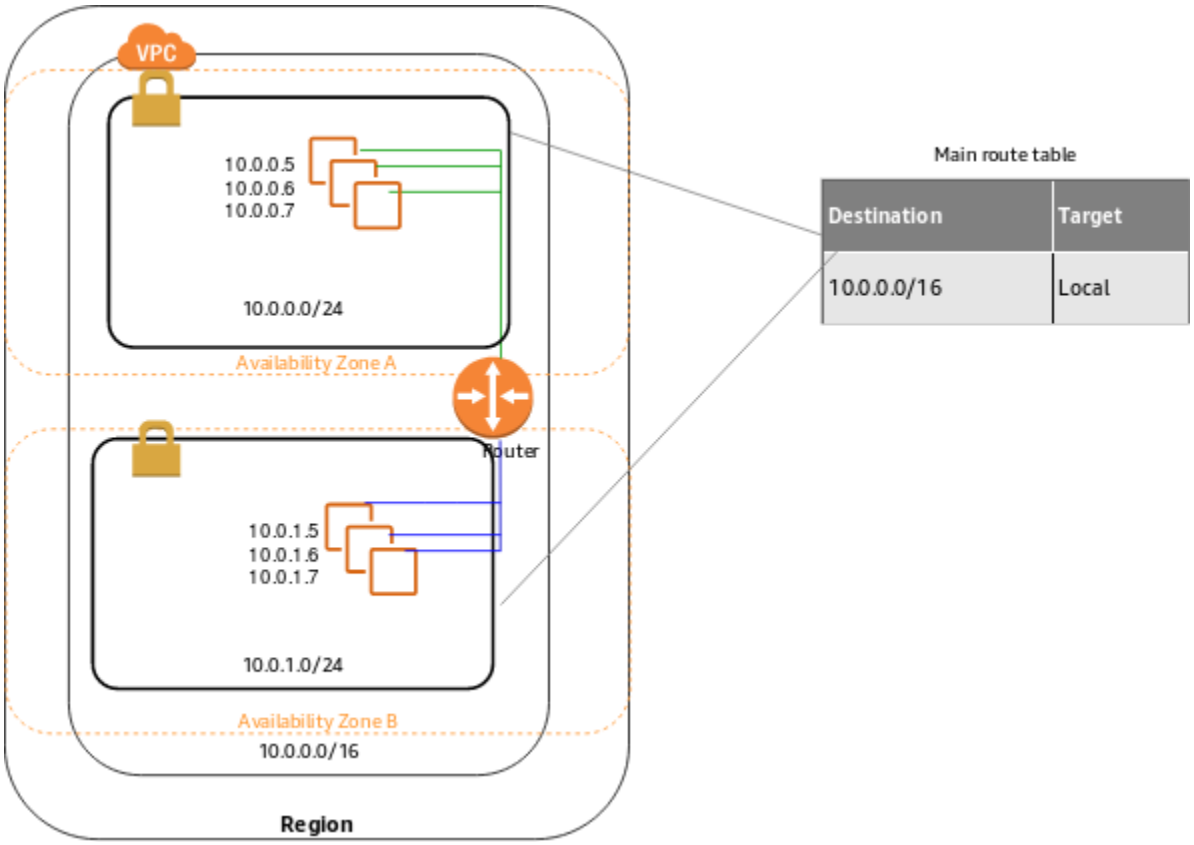
Acessar a Internet

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

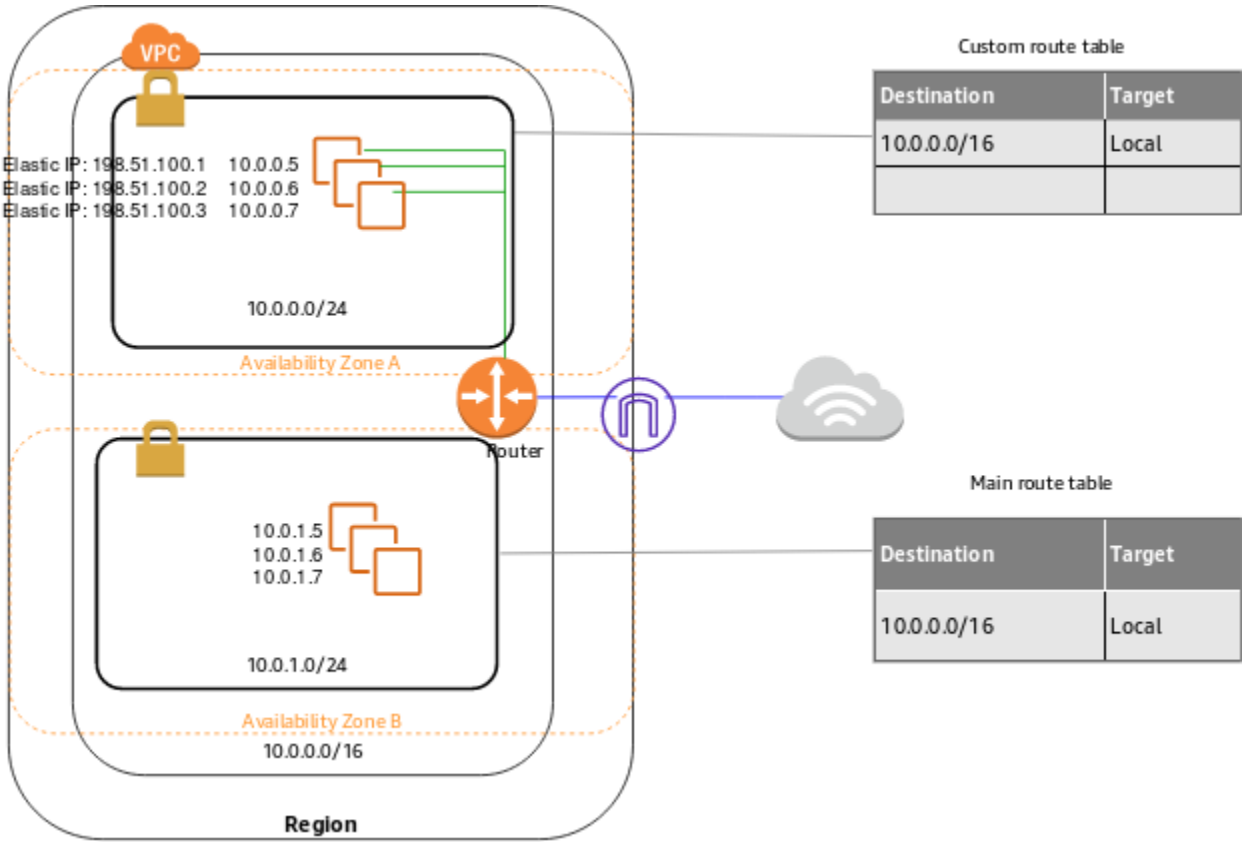
A VPC padrão inclui um gateway da Internet. Cada sub-rede padrão é uma sub-rede pública. Cada instância executada em uma sub-rede padrão possui dois endereços IPv4: um público e outro privado. Essas instâncias podem se comunicar com a Internet através do gateway da Internet. Um gateway da Internet permite 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 endereço de rede) para o tráfego IPv4. O NAT mapeia vários endereços IPv4 privados para um único endereço público IPv4. Um dispositivo NAT possui um endereço IP elástico, conectando-se à Internet por meio de um gateway da Internet. Conecte uma instância de uma sub-rede privada à Internet por meio do dispositivo NAT, que roteia o tráfego da instância para o gateway da Internet, assim como 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.

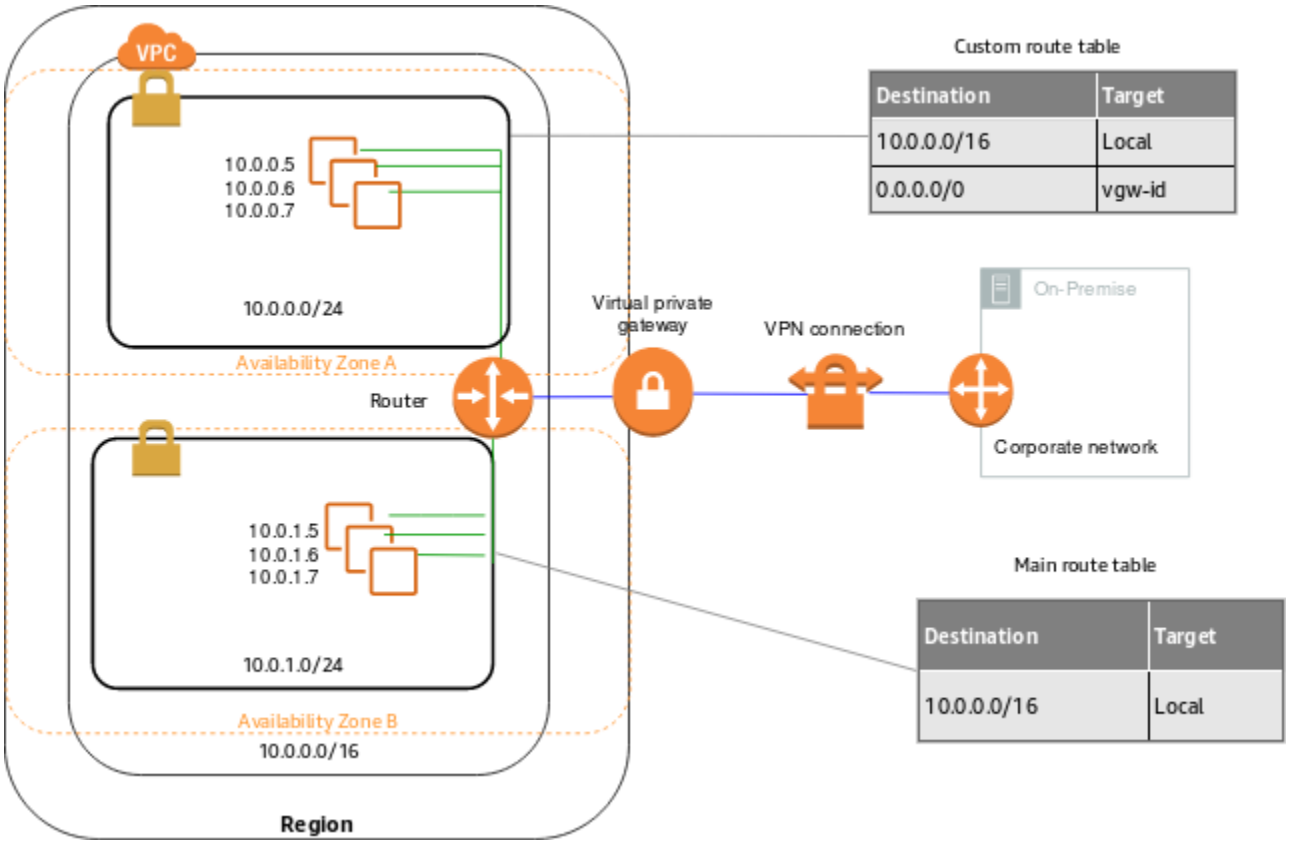
Mais informações

- Gateways da Internet (p. 212)
- Gateways da Internet apenas de saída (p. 218)
- Dispositivos NAT para sua VPC (p. 228)

Acessar uma rede corporativa ou doméstica

Você tem como opção conectar sua VPC ao seu próprio datacenter corporativo usando uma conexão do AWS Site-to-Site VPN IPsec, transformando a Nuvem AWS em uma extensão do seu datacenter.

Uma conexão do 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 no datacenter. Um dispositivo de gateway do cliente é um dispositivo físico ou um software configurado no seu lado da conexão do Site-to-Site VPN.



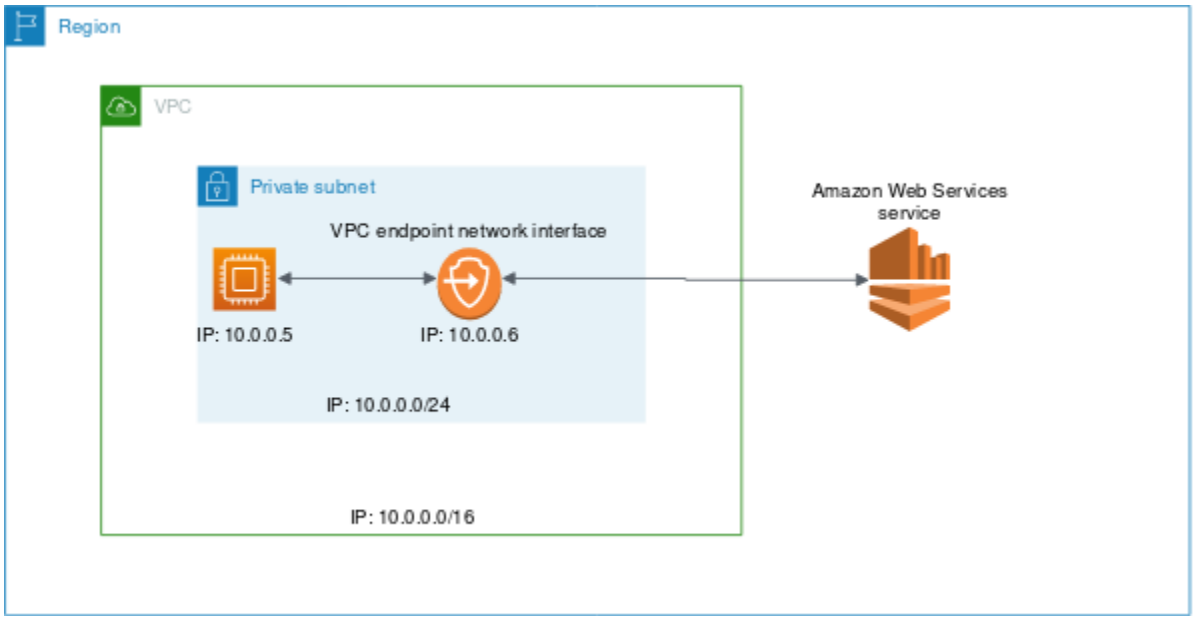
Mais informações

- Guia do usuário da AWS Site-to-Site VPN
- Transit Gateway

Acessar serviços pelo AWS PrivateLink

O AWS PrivateLink é uma tecnologia altamente disponível e escalável que permite a você conectar de forma privada sua VPC aos serviços compatíveis da AWS, a serviços hospedados por outras contas da AWS (serviços do VPC endpoint) e serviços compatíveis de parceiros do AWS Marketplace. Não é necessário ter um gateway da Internet, um dispositivo NAT, um endereço IP público, uma conexão do AWS Direct Connect ou uma conexão do AWS Site-to-Site VPN para se comunicar com o serviço. O tráfego entre sua VPC e o serviço não deixa a rede da Amazon.

Para usar o AWS PrivateLink, crie um VPC endpoint para um serviço na VPC. Crie o tipo de VPC endpoint necessário para o serviço compatível. Isso cria uma interface de rede elástica na sua sub-rede com um endereço IP privado que serve como ponto de entrada para o tráfego destinado ao serviço.



Você pode criar seu próprio serviço desenvolvido pelo AWS PrivateLink (serviço de endpoint) e permitir que outros clientes da AWS acessem seu serviço. Para obter mais informações, consulte o Guia do usuário do AWS PrivateLink.

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 no local. 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.

Mais informações

- Guia de emparelhamento de VPC
- Transit Gateway

Considerações sobre a rede global privada da AWS

A AWS fornece uma rede global privada de alto desempenho e baixa latência, que oferece um ambiente de computação em nuvem seguro para oferecer suporte às suas necessidades de redes. As regiões da AWS são conectadas a diversos provedores de serviços de Internet (ISPs), bem como a um backbone da rede global privada, que fornece um desempenho 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 nas 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) no backbone 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%.

Plataformas compatíveis

A versão original de Amazon EC2 era compatível com uma rede única que é compartilhada com outros clientes, designada como plataforma EC2-Classic. As contas da AWS anteriores ainda oferecem suporte a essa plataforma e podem executar as instâncias tanto no EC2-Classic como em uma VPC. As contas criadas após 04/12/2013 oferecem suporte somente para EC2-VPC. Para obter mais informações, consulte EC2-Classic no Guia do usuário do Amazon EC2 para instâncias do Linux.

Recursos da Amazon VPC

A tabela a seguir lista os recursos adicionais que podem ser úteis quando se trabalha com a Amazon VPC.

Recurso	Descrição
Opções de conectividade da Amazon Virtual Private Cloud	Fornece uma visão geral das opções de conectividade na rede.
Guia de emparelhamento de VPC	Descreve os cenários de conexões emparelhadas de VPC e as configurações de emparelhamento compatíveis.
Espelhamento de tráfego	Descreve destinos, filtros e sessões do espelhamento de tráfego e ajuda os administradores a configurá-los.
Transit Gateway	Descreve os gateways de trânsito e ajuda os administradores de rede a configurá-los.
Guia do gerenciador de rede do Transit Gateway	Descreve o gerenciador de rede do Transit Gateway e ajuda a configurar e monitorar uma rede global
Guia do usuário do AWS Direct Connect	Descreve como usar o AWS Direct Connect para criar uma conexão privada dedicada de uma rede remota para a VPC.
Guia do administrador da AWS Client VPN	Descreve como criar e configurar um endpoint de VPN cliente para permitir que usuários remotos acessem recursos em uma VPC.
Fórum da Amazon VPC	Um fórum baseado na comunidade para debater questões técnicas relacionadas à Amazon VPC.
Centro de recursos de conceitos básicos	Informações para ajudar nos conceitos básicos da compilação na AWS.
AWS Support Center	A página inicial do AWS Support.
Entre em contato conosco	Um ponto central de contato para dúvidas a respeito de faturamento, contas e eventos da AWS.

Conceitos básicos da Amazon VPC

Para começar a usar a Amazon VPC, é possível criar uma VPC não padrão. As etapas a seguir descrevem como usar o assistente da Amazon VPC para criar uma VPC não padrão com uma sub-rede pública, que é uma sub-rede que tem acesso à Internet por meio de um gateway da Internet. Depois, você poderá executar uma instância na sub-rede e conectar-se a ela.

Como alternativa, para começar a executar uma instância na VPC padrão existente, consulte Executar uma instância do EC2 na VPC padrão.

Antes de usar a Amazon VPC pela primeira vez, é necessário se cadastrar na Amazon Web Services (AWS). Ao se cadastrar, sua conta da AWS é automaticamente habilitada para todos os serviços da AWS, inclusive a Amazon VPC. Se ainda não criou uma conta da AWS, vá para https://aws.amazon.com/ e escolha Create a Free Account (Criar conta gratuita).

Se você pretende utilizar uma zona local para a VPC, crie uma VPC e, depois, crie uma sub-rede na zona local. Para obter mais informações, consulte the section called “Criar uma VPC” (p. 110) e the section called “Criar uma sub-rede na VPC” (p. 111).

Tópicos

Visão geral

Para concluir este exercício, faça o seguinte:

- Crie uma VPC não padrão com uma única sub-rede pública.
- Execute uma instância do Amazon EC2 na sub-rede.
- Associe um endereço IP elástico à sua instância. Isso permite que a instância acesse a Internet.

Para obter mais informações sobre como conceder permissões aos usuários do IAM para trabalhar com a Amazon VPC, consulte Identity and Access Management para o Amazon VPC (p. 162) e Exemplos de políticas da Amazon VPC (p. 170).

Etapa 1: criar a VPC

Nesta etapa, você usará o assistente da Amazon VPC do console da Amazon VPC para criar uma VPC. O assistente realizará as seguintes etapas para você:

- Cria uma VPC com um bloco CIDR IPv4 de tamanho /16 (uma rede com 65.536 endereços IP privados).
- Anexa um gateway da Internet à VPC.
- Cria uma sub- rede IPv4 de tamanho /24 (um intervalo de 256 endereços IP privados) na VPC.

- Cria uma tabela de rotas personalizada e a associa à sua sub-rede para que o tráfego possa fluir entre a sub-rede e o gateway da Internet.

Como criar uma VPC usando o assistente da Amazon VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. Na barra de navegação, na parte superior direita, anote a região da AWS em que você estará criando a VPC. Certifique-se de continuar trabalhando na mesma região no restante do exercício, porque não será possível iniciar uma instância em sua VPC de uma região diferente.
3. No painel de navegação, escolha VPC dashboard (Painel da VPC). No painel, selecione Launch VPC Wizard (Iniciar assistente da VPC).

   Note

   Não escolha Your VPCs (Suas VPCs) no painel de navegação; você não pode acessar o assistente da VPC usando o botão Create VPC (Criar VPC) nessa página.
4. Selecione VPC com uma única sub-rede pública e Selecionar.
5. No painel de configuração, digite um nome para a VPC no campo VPC name; por exemplo, `my-vpc` e digite um nome para sua sub-rede no campo Sub-rede name. Isso ajuda você a identificar a VPC e a sub-rede no console da Amazon VPC depois que são criadas. Para este exercício, deixe as outras definições de configuração na página e escolha Criar VPC.
6. Uma janela de status mostra o trabalho em andamento. Quando o trabalho for concluído, escolha OK para fechar a janela de status.
7. A página Your VPCs exibe sua VPC padrão e a VPC que você acabou de criar. A VPC que você criou é uma VPC não padrão, portanto a coluna Default VPC exibe Não.

Visualizar informações sobre sua VPC

Depois que criar a VPC, você poderá ver informações sobre a sub-rede, o gateway da Internet e as tabelas de rotas. A VPC criada possui duas tabelas de rotas: uma tabela de rotas principal, que todas as VPCs possuem por padrão, e uma tabela de rotas personalizada criada pelo assistente. A tabela de rotas personalizada é associada à sua sub-rede, o que significa que as rotas nessa tabela determinam como o tráfego flui para a sub-rede. Se você adicionar uma nova sub-rede à VPC, a tabela de rota principal será usada como padrão.

Para visualizar informações sobre sua VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Your VPCs (Suas VPCs). Anote o nome e o ID da VPC que você criou (veja nas colunas Nome e VPC ID). Você usará essas informações para identificar os componentes que estão associados à sua VPC.
3. No painel de navegação, escolha Sub-redes. O console exibe a sub-rede que foi criada quando você criou sua VPC. Você pode identificar a sub-rede pelo seu nome na coluna Nome ou pode usar as informações da VPC que você obteve na etapa anterior e procurar na coluna VPC.
4. No painel de navegação, escolha Gateways da Internet. É possível encontrar o gateway da Internet que está anexado à sua VPC procurando na coluna VPC, que exibe o ID e o nome (se aplicável) da VPC.
5. No painel de navegação, escolha Route Tables. Há duas tabelas de rotas associadas à VPC. Selecione a tabela de rotas personalizada (a coluna Main exibe Não) e escolha a tabela Rotas para exibir as informações de rotas no painel de detalhes:

   - A primeira linha na tabela é a rota local, que permite instâncias na VPC para comunicar. Essa rota está presente em todas as tabelas de rotas por padrão e não pode ser removida.

- A segunda linha mostra a rota que o assistente da Amazon VPC adicionou para permitir que o tráfego destinado à Internet (`0.0.0.0/0`) flua da sub-rede para o gateway da Internet.

6. Selecione a tabela de rota principal. A tabela de rota principal tem uma rota local, mas não há outras rotas.

Etapa 2: executar uma instância em sua VPC

Quando iniciar uma instância do EC2 em uma VPC, especifique a sub-rede na qual iniciar a instância. Neste caso, você iniciará uma instância na sub-rede pública da VPC que criou. Você usará o assistente de execução do Amazon EC2 no console do Amazon EC2 para executar a instância.

Para executar uma instância do EC2 em uma VPC

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação na parte superior direita da tela, certifique-se de selecionar a mesma região em que você criou a VPC.
3. No painel, escolha Launch Instance (Executar instância).
4. Na primeira página do assistente, escolha a AMI que deseja usar. Para este exercício, escolha uma AMI do Amazon Linux ou uma AMI do Windows.
5. Na página Choose an Instance Type, você pode selecionar a configuração do hardware e o tamanho da instância a ser executada. Por padrão, o assistente seleciona o primeiro tipo de instância disponível com base na AMI que você selecionou. Você pode deixar a seleção padrão e escolher Next: Configure Instance Details.
6. Na página Configure Instance Details, selecione a VPC que você criou na lista Rede e a sub-rede na lista Sub-rede. Deixe o resto das configurações padrão e percorra as páginas seguintes do assistente até chegar à página Add Tags.
7. Na página Add Tags, você pode marcar sua instância com uma tag `Name`, por exemplo, `Name=MyWebServer`. Isso ajuda você a identificar sua instância no console do Amazon EC2 depois de executá-la. Escolha Next: Configure Security Group (Próximo: configurar grupo de segurança) ao concluir.
8. Na página Configure Security Group (Configurar security group), o assistente automaticamente define o security group x do assistente de lançamento para permitir que você se conecte à sua instância. Escolha Review and Launch.

   Important

   O assistente cria uma regra de grupo de segurança que permite que todos os endereços IP (`0.0.0.0/0`) acessem sua instância usando SSH ou RDP. Isso é aceitável para um exercício rápido, mas não é seguro para ambientes de produção. Na produção, você autorizará apenas um endereço IP específico ou intervalo de endereços para acessar a instância.

9. Na página Review Instance Launch, escolha Launch.
10. Na caixa de diálogo Select an existing key pair or create a new key pair (Selecionar um par de chaves existente ou criar um novo par de chaves), você poderá escolher um par de chaves existente ou poderá criar um novo. Se criar um novo par de chaves, assegure-se de baixar e armazenar o arquivo em um local seguro. Você precisará do conteúdo da chave privada para conectar-se à sua instância depois que ela for executada.

    Para executar uma instância, marque a caixa de seleção de confirmação e escolha Iniciar instâncias.
11. Na página de confirmação, escolha View Instances para visualizar a instância na página Instâncias. Selecione sua instância e visualize seus detalhes na guia Description. O campo Private IPs exibe o endereço IP privado atribuído à sua instância no intervalo de endereços IP da sua sub-rede.

Para obter mais informações sobre as opções disponíveis no assistente de execução do Amazon EC2, consulte Executar uma instância no Guia do usuário do Amazon EC2 para instâncias do Linux.

Etapa 3: atribuir um endereço IP elástico à instância

Na etapa anterior, você executou a instância em uma sub-rede pública: uma sub-rede que tem uma rota para um gateway da Internet. No entanto, a instância na sub-rede também precisa de um endereço IPv4 público para se comunicar com a Internet. Como padrão, uma instância em uma VPC não padrão não recebe um endereço IPv4 público. Nesta etapa, você alocará um endereço IP elástico à sua conta e o associará à sua instância.

Para alocar e atribuir um endereço Elastic IP

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 Allocate new address (Alocar novo endereço) e, em seguida, Allocate, (Alocar).
4. Selecione o endereço IP elástico na lista, selecione Actions (Ações) e Associate address (Associar endereço).
5. Para Resource type (Tipo de recurso), verifique se Instance (Instância) está selecionada. Escolha sua instância na lista Instance (Instância). Escolha Associate (Associar) ao concluir.

A instância agora é acessível pela Internet. Você pode se conectar à instância pelo endereço IP elástico usando SSH ou área de trabalho remota de sua rede doméstica. Para obter mais informações sobre como se conectar a uma instância do Linux, consulte Conectar-se à instância do Linux no Guia do usuário do Amazon EC2 para instâncias do Linux. Para obter mais informações sobre como se conectar a uma instância do Windows, consulte Conectar-se à instância do Windows no Guia do usuário do Amazon EC2 para instâncias do Windows.

Etapa 4: Limpeza

Você pode optar por continuar usando a instância na sua VPC ou, se não precisar dela, encerre-a e libere seu endereço IP elástico para evitar novas cobranças. Também é possível excluir a VPC: observe que a VPC e os componentes de VPC criados neste exercício não são cobrados (como sub-redes e tabelas de rotas).

Antes de excluir a VPC, é preciso finalizar as instâncias em execução na VPC. Será possível então excluir a VPC e os componentes dela usando o console da VPC.

Para concluir a instância, libere o endereço IP elástico e exclua sua VPC

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, escolha Ações, Instance State e Terminate.
4. Na caixa de diálogo, expanda a seção Release attached Elastic IPs e marque a caixa de seleção próxima ao endereço IP elástico. Escolha Yes, Terminate.
5. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
6. No painel de navegação, selecione Your VPCs (Suas VPCs).
7. Selecione a VPC, escolha Ações e Delete VPC.

8. Quando a confirmação for solicitada, escolha Delete VPC (Excluir VPC).

Próximas etapas

Depois de criar uma VPC não padrão, faça o seguinte:

- Adicione mais sub-redes à sua VPC. Para obter mais informações, consulte Criar uma sub-rede na VPC (p. 111).
- Habilite o suporte IPv6 para a VPC e as sub-redes. Para obter mais informações, consulte Associar um bloco CIDR IPv6 à sua VPC (p. 113) e Associar um bloco CIDR IPv6 à sub-rede (p. 114).
- Habilite instâncias em uma sub-rede privada para acessar a Internet. Para obter mais informações, consulte Dispositivos NAT para sua VPC (p. 228).

Conceitos básicos do IPv6 para Amazon VPC

As etapas a seguir descrevem como criar uma VPC não padrão que ofereça suporte ao endereçamento IPv6.

Para concluir este exercício, faça o seguinte:

- Crie uma VPC não padrão com um bloco CIDR IPv6 e uma única sub-rede pública. As sub-redes permitem que você agrupe instâncias com base em suas necessidades operacionais e de segurança. Uma sub-rede pública é uma sub-rede que tem acesso à Internet por um gateway da Internet.
- Crie um security group para sua instância que permita o tráfego somente por portas específicas.
- Execute uma instância do Amazon EC2 na sub-rede e associe um endereço IPv6 à instância durante a execução. Um endereço IPv6 é globalmente exclusivo e permite que sua instância se comunique com a Internet.
- É possível solicitar um bloco CIDR IPv6 para a VPC. Ao selecionar essa opção, defina o grupo de borda de rede, que é o local do qual anunciamos o bloco CIDR IPV6. Definir o grupo de borda de rede limita o bloco CIDR a este grupo.

Para obter mais informações sobre o endereçamento IPv4 e IPv6, consulte Endereçamento IP na VPC.

Se você pretende utilizar uma zona local para a VPC, crie uma VPC e, depois, crie uma sub-rede na zona local. Para obter mais informações, consulte the section called “Criar uma VPC” (p. 110) e the section called “Criar uma sub-rede na VPC” (p. 111).

Tarefas

- Etapa 1: criar a VPC (p. 15)
- Etapa 2: Criar um grupo de segurança (p. 18)
- Etapa 3: Executar uma instância (p. 19)

Etapa 1: criar a VPC

Nesta etapa, use o assistente da Amazon VPC do console da Amazon VPC para criar uma VPC. Por padrão, o assistente realizará as seguintes etapas para você:

- Cria uma VPC com um bloco CIDR IPv4 /16 e associa um bloco CIDR IPv6 /56 à VPC. Para obter mais informações, consulte Sua VPC. O tamanho do bloco CIDR IPv6 é fixo (/ 56) e a variedade de endereços IPv6 é alocada automaticamente do grupo de endereços IPv6 da Amazon (não é permitido que você mesmo faça a seleção).

- Anexa um gateway da Internet à VPC. Para obter mais informações sobre gateways da Internet, consulte Gateways da Internet.
- Cria uma sub-rede com um bloco CIDR IPv4 /24 e um bloco CIDR IPv6 /64 na VPC. O tamanho do bloco CIDR IPv6 é fixo (/64).
- Cria uma tabela de rotas personalizada e a associa à sua sub-rede para que o tráfego possa fluir entre a sub-rede e o gateway da Internet. Para obter mais informações sobre tabelas de rotas, consulte Tabelas de rotas.
- Associa um bloco CIDR IPv6 fornecido pela Amazon a um grupo de borda de rede. Para obter mais informações, consulte the section called “Estender os recursos da VPC para zonas locais” (p. 143).

> **Note**
>
> Este exercício abrange o primeiro cenário no assistente de VPC. Para obter mais informações sobre outros cenários, consulte Cenários da Amazon VPC.

Como criar uma VPC na zona de disponibilidade padrão

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. Na barra de navegação, no canto superior direito, escolha a região em que deseja criar a VPC. Certifique-se de continuar trabalhando na mesma região no restante do exercício, porque não será possível iniciar uma instância em sua VPC de uma região diferente. Para obter mais informações, consulte Regiões e zonas de disponibilidade no Guia do usuário do Amazon EC2 para instâncias do Linux.
3. No painel de navegação, selecione VPC dashboard (Painel da VPC) e Launch VPC Wizard (Iniciar assistente da VPC).

   > **Note**
   >
   > Não escolha Your VPCs (Suas VPCs) no painel de navegação; você não pode acessar o assistente da VPC usando o botão Create VPC (Criar VPC) nessa página.
4. Escolha a opção para a configuração que deseja implementar, por exemplo, VPC with a Single Public Subnet (VPC com uma única sub-rede pública) e selecione Select (Selecionar).
5. Na página de configuração, insira um nome para a VPC no campo VPC name; por exemplo, `my-vpc` e insira um nome para sua sub-rede no campo Sub-rede name. Isso ajuda você a identificar a VPC e a sub-rede no console da Amazon VPC depois que são criadas.
6. Em IPv4 CIDR block (Bloco CIDR IPv4), mantenha a configuração padrão (`10.0.0.0/16`) ou especifique sua própria. Para obter mais informações, consulte Dimensionamento da VPC.

   No bloco CIDR IPv6, escolha Amazon-provided IPv6 CIDR block.
7. Em Public subnet's IPv4 CIDR, deixe a configuração padrão ou especifique a sua. Em Public subnet's IPv6 CIDR, escolha Specify a custom IPv6 CIDR. Você pode deixar o valor do par hexadecimal padrão para a sub-rede IPv6 (`00`).
8. Mantenha o restante das configurações padrão da página e escolha Create VPC.
9. Uma janela de status mostra o trabalho em andamento. Quando o trabalho for concluído, escolha OK para fechar a janela de status.
10. A página Your VPCs exibe sua VPC padrão e a VPC que você acabou de criar.

Como criar uma VPC em uma região local

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. Na barra de navegação, no canto superior direito, escolha a região em que deseja criar a VPC. Certifique-se de continuar trabalhando na mesma região no restante do exercício, porque não será possível iniciar uma instância em sua VPC de uma região diferente. Para obter mais informações,

consulte Regiões e zonas de disponibilidade no Guia do usuário do Amazon EC2 para instâncias do Linux.

3. No painel de navegação, selecione VPC dashboard (Painel da VPC) e Launch VPC Wizard (Iniciar assistente da VPC).

   Note

   Não escolha Your VPCs (Suas VPCs) no painel de navegação; você não pode acessar o assistente da VPC usando o botão Create VPC (Criar VPC) nessa página.
4. Escolha a opção para a configuração que deseja implementar, por exemplo, VPC with a Single Public Subnet (VPC com uma única sub-rede pública) e selecione Select (Selecionar).
5. Na página de configuração, insira um nome para a VPC no campo VPC name; por exemplo, `my-vpc` e insira um nome para sua sub-rede no campo Sub-rede name. Isso ajuda você a identificar a VPC e a sub-rede no console da Amazon VPC depois que são criadas.
6. Em IPv4 CIDR block (Bloco CIDR IPv4), especifique o bloco CIDR. Para obter mais informações, consulte Dimensionamento da VPC.
7. No bloco CIDR IPv6, escolha Amazon-provided IPv6 CIDR block.
8. Em Network Border Group (Grupo de borda de rede), escolha o grupo de onde a AWS anuncia os endereços IP.
9. Mantenha o restante das configurações padrão da página e escolha Create VPC.
10. Uma janela de status mostra o trabalho em andamento. Quando o trabalho for concluído, escolha OK para fechar a janela de status.
11. A página Your VPCs exibe sua VPC padrão e a VPC que você acabou de criar.

Visualizar informações sobre a VPC

Depois de criar a VPC, você pode visualizar informações sobre sub-rede, gateway da Internet e tabelas de rotas. A VPC criada possui duas tabelas de rotas: uma tabela de rotas principal, que todas as VPCs possuem por padrão, e uma tabela de rotas personalizada criada pelo assistente. A tabela de rotas personalizada é associada à sua sub-rede, o que significa que as rotas nessa tabela determinam como o tráfego flui para a sub-rede. Se você adicionar uma nova sub-rede à VPC, a tabela de rota principal será usada como padrão.

Para visualizar informações sobre sua VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Your VPCs (Suas VPCs). Anote o nome e o ID da VPC que você criou (veja nas colunas Nome e VPC ID). Você usará essas informações para identificar os componentes que estão associados à sua VPC.

   Ao usar zonas locais, a entrada IPv6 (Grupo de borda de rede) indica o grupo de borda de rede da VPC (por exemplo, `us-west-2-lax-1`).
3. No painel de navegação, escolha Sub-redes. O console exibe a sub-rede que foi criada quando você criou sua VPC. Você pode identificar a sub-rede pelo seu nome na coluna Nome ou pode usar as informações da VPC que você obteve na etapa anterior e procurar na coluna VPC.
4. No painel de navegação, escolha Gateways da Internet. É possível encontrar o gateway da Internet que está anexado à sua VPC procurando na coluna VPC, que exibe o ID e o nome (se aplicável) da VPC.
5. No painel de navegação, escolha Route Tables. Há duas tabelas de rotas associadas à VPC. Selecione a tabela de rotas personalizada (a coluna Main exibe Não) e escolha a tabela Rotas para exibir as informações de rotas no painel de detalhes:

   - As duas primeiras linhas na tabela são as rotas locais, que permitem que instâncias dentro da VPC se comuniquem via IPv4 e IPv6. Não é possível remover essas rotas.

- A linha seguinte mostra a rota que o assistente da Amazon VPC adicionou para permitir que o tráfego destinado a um endereço IPv4 fora da VPC (`0.0.0.0/0`) flua da sub-rede para o gateway da Internet.
- A linha seguinte mostra a rota que permite que o tráfego destinado a um endereço IPv6 fora da VPC (`::/0`) flua da sub-rede para o gateway da Internet.

6. Selecione a tabela de rota principal. A tabela de rota principal tem uma rota local, mas não há outras rotas.

Etapa 2: Criar um grupo de segurança

Um security group atua como firewall virtual que controla o tráfego de suas instâncias associadas. Para usar um security group, adicione as regras de entrada para controlar o tráfego que entra na instância e as regras de saída para controlar o tráfego que sai da instância. Para associar um security group a uma instância, especifique o security group quando iniciar a instância.

Sua VPC é fornecida com um security group padrão. Qualquer instância que, ao iniciar, não for associada a outro security group, será associada ao security group padrão. Neste exercício, você criará um novo security group `WebServerSG` que será especificado no início de uma instância na sua VPC.

Criar o seu grupo de segurança WebServerSG

É possível criar o grupo de segurança usando o console da Amazon VPC.

Para criar o security group WebServerSG e adicionar regras

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Security groups, Criar security group.
3. Em Group name, insira `WebServerSG` como o nome do security group e forneça uma descrição. Você pode, opcionalmente, usar o campo Name tag para criar uma tag para o security group com uma chave do `Name` e um valor que você especificar.
4. Selecione o ID de sua VPC no menu VPC e escolha Yes, Create.
5. Selecione o security group `WebServerSG` que acabou de criar (você pode visualizar seu nome na coluna Group Name).
6. Na guia Inbound Rules, escolha Edit e adicione regras para tráfego de entrada da seguinte forma:
   a. Em Type, escolha HTTP e insira `::/0` no campo Source.
   b. Escolha Add another rule. Em Type, escolha HTTPS e insira `::/0` no campo Source.
   c. Escolha Add another rule. Se estiver iniciando uma instância Linux, escolha SSH em Type ou, se estiver iniciando uma instância Windows, escolha RDP. Insira o intervalo de endereços IPv6 públicos da rede no campo Source. Se não souber este intervalo de endereços, você poderá usar `::/0` para este exercício.

      Important

      Ao usar o `::/0`, você permite que todos os endereços IPv6 acessem sua instância usando o SSH ou o RDP. Isso é aceitável para um exercício rápido, mas não é seguro para ambientes de produção. Na produção, autorize apenas um endereço IP específico ou um intervalo de endereços para acessar a instância.

   d. Escolha Salvar.

Etapa 3: Executar uma instância

Quando iniciar uma instância do EC2 em uma VPC, especifique a sub-rede na qual iniciar a instância. Neste caso, você iniciará uma instância na sub-rede pública da VPC que criou. Use o assistente de execução do Amazon EC2 no console do Amazon EC2 para executar a instância.

Para garantir que a instância seja acessível pela Internet, atribua à instância um endereço IPv6 do intervalo de sub-redes durante a execução. Isso garante que a instância possa se comunicar com a Internet via IPv6.

Para executar uma instância do EC2 em uma VPC

Antes de executar a instância do EC2 na VPC, configure a sub-rede da VPC para atribuir endereços IPv6 automaticamente. Para obter mais informações, consulte the section called “Modificar o atributo de endereçamento IPv6 para a sub-rede” (p. 122).

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação na parte superior direita da tela, certifique-se de selecionar a mesma região em que você criou a VPC e o grupo de segurança.
3. No painel, escolha Launch Instance (Executar instância).
4. Na primeira página do assistente, escolha a AMI que deseja usar. Para este exercício, recomendamos que escolha uma AMI do Amazon Linux ou do Windows.
5. Na página Choose an Instance Type, você pode selecionar a configuração do hardware e o tamanho da instância a ser executada. Por padrão, o assistente seleciona o primeiro tipo de instância disponível com base na AMI que você selecionou. Você pode deixar a seleção padrão e escolher Next: Configure Instance Details.
6. Na página Configure Instance Details, selecione a VPC que você criou na lista Rede e a sub-rede na lista Sub-rede.
7. Em Auto-assign IPv6 IP, escolha Habilitar.
8. Deixe o resto das configurações padrão e percorra as páginas seguintes do assistente até chegar à página Add Tags.
9. Na página Add Tags, você pode marcar sua instância com uma tag `Name`, por exemplo, `Name=MyWebServer`. Isso ajuda você a identificar sua instância no console do Amazon EC2 depois de executá-la. Escolha Next: Configure Security Group (Próximo: configurar grupo de segurança) ao concluir.
10. Na página Configure Security Group (Configurar security group), o assistente automaticamente define o security group x do assistente de lançamento para permitir que você se conecte à sua instância. Em vez disso, escolha a opção Select an existing security group, selecione o grupo WebServerSG que criou anteriormente e escolha Review and Launch.
11. Na página Review Instance Launch, verifique os detalhes da instância e escolha Launch.
12. Na caixa de diálogo Select an existing key pair or create a new key pair (Selecionar um par de chaves existente ou criar um novo par de chaves), você poderá escolher um par de chaves existente ou poderá criar um novo. Se criar um novo par de chaves, assegure-se de baixar e armazenar o arquivo em um local seguro. Você precisará do conteúdo da chave privada para conectar-se à sua instância depois que ela for executada.

    Para executar uma instância, selecione a caixa de seleção de confirmação e escolha Iniciar instâncias.
13. Na página de confirmação, escolha View Instances para visualizar a instância na página Instâncias. Selecione sua instância e visualize seus detalhes na guia Description. O campo Private IPs exibe o endereço IPv4 privado atribuído à instância no intervalo de endereços IPv4 da sub-rede. O campo Private IPs exibe o endereço IPv6 privado atribuído à instância no intervalo de endereços IPv6 da sub-rede.

Para obter mais informações sobre as opções disponíveis no assistente de execução do Amazon EC2, consulte Executar uma instância no Guia do usuário do Amazon EC2 para instâncias do Linux.

Você pode se conectar à instância pelo endereço IPv6 elástico usando SSH ou área de trabalho remota a partir de sua rede doméstica. Seu computador local deve ter um endereço IPv6 e configurado para usar IPv6. Para obter mais informações sobre como se conectar a uma instância do Linux, consulte Conectar-se à instância do Linux no Guia do usuário do Amazon EC2 para instâncias do Linux. Para obter mais informações sobre como se conectar a uma instância do Windows, consulte Conectar-se à instância do Windows usando RDP no Guia do usuário do Amazon EC2 para instâncias do Windows.

> Note
>
> Se você também deseja que a instância seja acessível a partir de um endereço IPv4 via Internet, SSH ou RDP, você deve associar um endereço IP Elástico (um endereço IPv4 público estático) à instância e ajustar as regras do grupo de segurança para permitir acesso via IPv4. Para obter mais informações, consulte Conceitos básicos da Amazon VPC (p. 11).

Configurações do assistente de console da Amazon VPC

É possível usar o assistente de console da Amazon VPC para criar uma das seguintes configurações de VPC não padrão.

Tópicos

VPC com uma única sub-rede pública

A configuração deste cenário inclui uma nuvem privada virtual (VPC) com uma única sub-rede pública e um gateway da Internet para permitir a comunicação pela Internet. Recomendamos esta configuração se você precisar executar um aplicativo da web de única camada voltado para o público, como um blog ou um site simples.

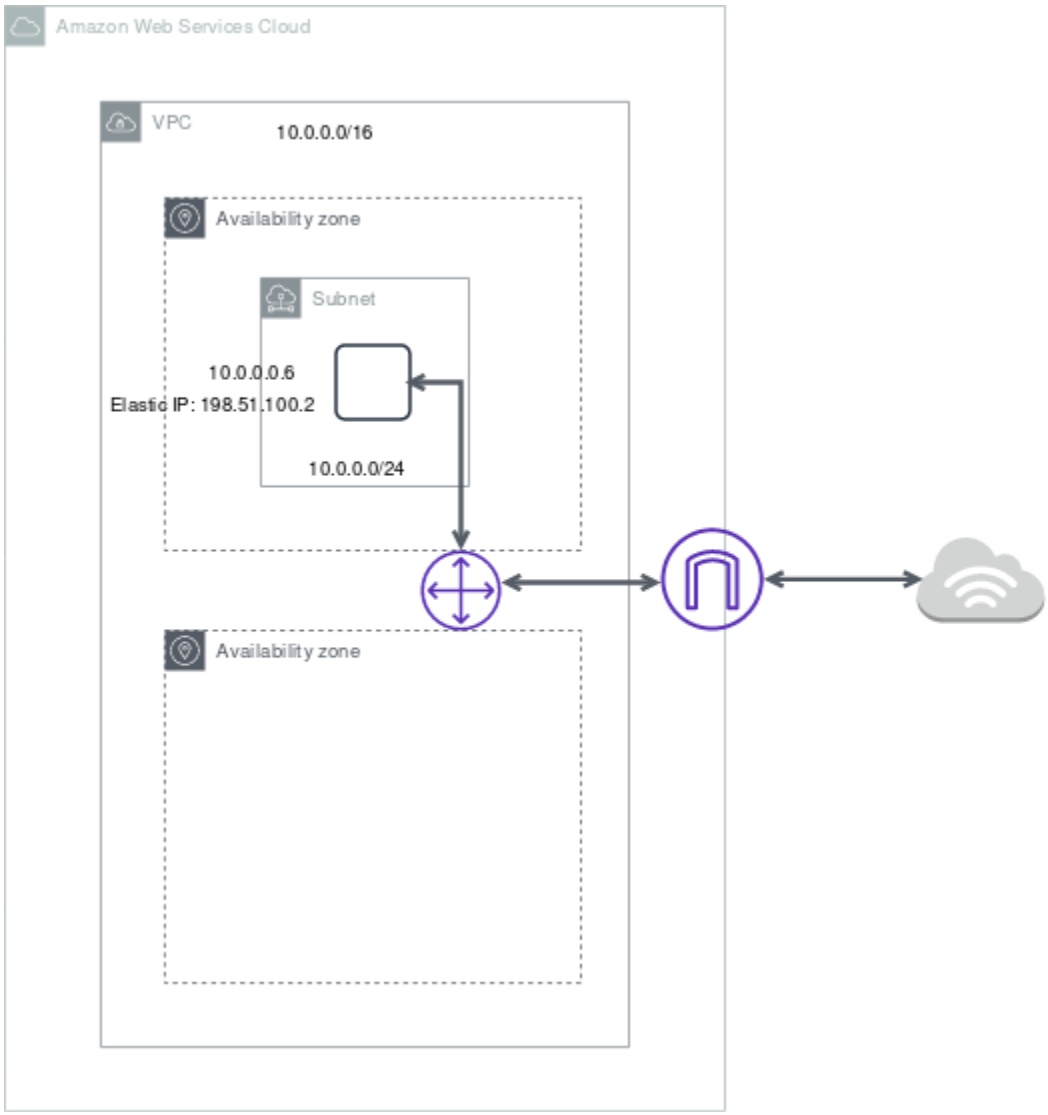
Além disso, este cenário pode ser opcionalmente configurado para IPv6: é possível usar o assistente de VPC para criar uma VPC e uma sub-rede com blocos CIDR IPv6 associados. As instâncias iniciadas em sub-redes públicas podem receber endereços IPv6 e se comunicar usando IPv6. Para obter mais informações sobre endereçamento IPv4 e IPv6, consulte Endereçamento IP na sua VPC (p. 117).

Para obter informações sobre como gerenciar o software de instância do EC2, consulte Gerenciar software na instância do Linux no Guia do usuário do Amazon EC2 para instâncias do Linux.

Tópicos

Visão geral

O diagrama a seguir mostra os principais componentes da configuração deste cenário.



Note

Se tiver concluído Conceitos básicos da Amazon VPC (p. 11), você já terá implementado esse cenário usando o assistente da VPC no console da Amazon VPC.

A configuração deste cenário inclui o seguinte:

- Uma nuvem privada virtual (VPC) com um bloco CIDR IPv4 tamanho /16 (exemplo: 10.0.0.0/16). Nesse caso, são fornecidos 65.536 endereços IPv4.
- Uma sub-rede com bloco CIDR IPv4 tamanho /24 (exemplo: 10.0.0.0/24). Nesse caso, são fornecidos 256 endereços IPv4.
- Um gateway de internet. Isso conecta a VPC à Internet e a outros serviços da AWS.
- Uma instância com um endereço IPv4 privado em um intervalo de sub-rede (exemplo: 10.0.0.6), que permite à instância se comunicar com outras instâncias na VPC, e um endereço IPv4 elástico (exemplo: 198.51.100.2), que é um endereço IPv4 público que permite à instância se conectar à Internet e ser alcançada na Internet.
- Uma tabela de rotas personalizada associada à sub-rede. As entradas da tabela de rotas permitem que as instâncias na sub-rede usem o IPv4 para se comunicarem com outras instâncias na VPC e para se

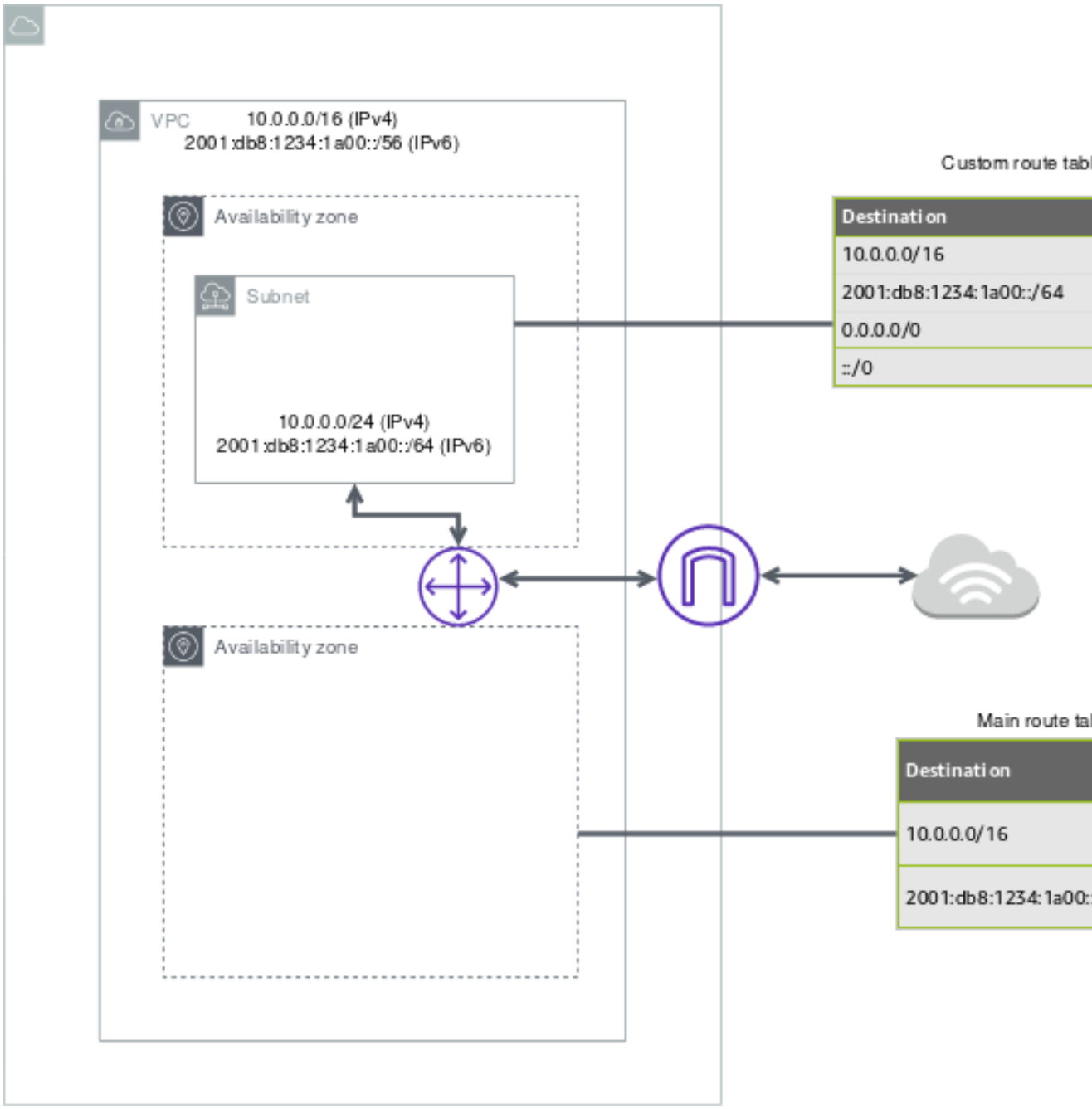
comunicarem diretamente pela Internet. Uma sub-rede associada a uma tabela de rotas que tenha uma rota para um gateway da Internet é conhecida como sub-rede pública.

Para obter mais informações sobre sub-redes, consulte VPCs e sub-redes (p. 100). Para obter mais informações sobre gateways da Internet, consulte Gateways da Internet (p. 212).

Visão geral de IPv6

Opcionalmente, você pode ativar o IPv6 para este cenário. Além dos componentes listados anteriormente, a configuração inclui o seguinte:

- Um bloco CIDR IPv6 tamanho /56 associado à VPC (exemplo: 2001:db8:1234:1a00::/56). A Amazon atribui automaticamente o CIDR; você não pode escolher o intervalo.
- Um bloco CIDR IPv6 tamanho /64 associado a uma sub-rede pública (exemplo: 2001:db8:1234:1a00::/64). Você pode escolher o intervalo para sua sub-rede com base no intervalo alocado à VPC. Você não pode escolher o tamanho do bloco CIDR IPv6 da sub-rede.
- Um endereço IPv6 atribuído a uma instância no intervalo da sub-rede (exemplo: 2001:db8:1234:1a00::123).
- Entradas da tabela de rotas na tabela de rotas personalizada que permitem às instâncias na VPC usarem IPv6 para se comunicarem entre si e diretamente pela Internet.



Roteamento

Sua VPC tem um roteador implícito (mostrado no diagrama de configuração acima). Neste cenário, o assistente de VPC cria uma tabela de rotas personalizada que encaminha todo o tráfego destinado a um endereço fora da VPC para o gateway da Internet e associa essa tabela de rotas à sub-rede.

A tabela a seguir mostra a tabela de rotas para o exemplo no diagrama de configuração acima. A primeira entrada é a padrão para um roteamento IPv4 local na VPC; essa entrada permite que as instâncias na VPC comuniquem-se entre si. A segunda entrada encaminha todos os outros tráfegos IPv4 da sub-rede para o gateway da Internet (por exemplo, `igw-1a2b3c4d`).

Destino	Destino
10.0.0.0/16	local
0.0.0.0/0	igw-id

Roteamento para o IPv6

Se você associar um bloco CIDR IPv6 à sua VPC e à sub-rede, a tabela de rotas incluirá rotas distintas para o tráfego IPv6. A tabela a seguir mostra a tabela de rotas personalizada para este cenário, se você escolher habilitar a comunicação IPv6 na sua VPC. A segunda entrada é a rota padrão adicionada automaticamente para roteamento local na VPC via IPv6. A quarta entrada roteia todos os outros tráfegos IPv6 da sub-rede para o gateway da Internet.

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

A AWS fornece dois recursos que você pode usar para aumentar a segurança da VPC: grupos de segurança e ACLs da rede. Os grupos de segurança controlam o tráfego de entrada e de saída de suas instâncias e as Network ACL controlam o tráfego de entrada e de saída de suas sub-redes. Na maioria dos casos, os grupos de segurança podem atender as suas necessidades; contudo, você também pode usar as Network ACL se desejar uma camada adicional de segurança para o seu VPC. Para obter mais informações, consulte Privacidade do tráfego entre redes na Amazon VPC (p. 158).

Para este cenário, você usará um security group, mas não uma rede ACL. Se quiser usar uma network ACL, consulte Regras de network ACL recomendadas para uma VPC com uma única sub-rede pública (p. 27).

Sua VPC é fornecida com um security group padrão (p. 181). Uma instância executada na VPC será automaticamente associada ao security group padrão se você não especificar um security group diferente durante a execução. É possível adicionar regras específicas ao grupo de segurança padrão, mas talvez não sejam adequadas para outras instâncias iniciadas na VPC. Em vez disso, recomendamos que crie um security group personalizado para o servidor da web.

Para este cenário, crie um security group chamado `WebServerSG`. Quando você cria um security group, ele possui apenas uma regra de saída que permite a todo o tráfego deixar as instâncias. Você deve modificar as regras para permitir o tráfego de entrada e para restringir o tráfego de saída, conforme necessário. Especifique este security group quando você iniciar instâncias na VPC.

A seguir, as regras de entrada e saída do tráfego IPv4 para o security group WebServerSG.

Entrada			
Origem	Protocolo	Intervalo de portas	Comentários

0.0.0.0/0	TCP	80	Permite acesso HTTP de entrada para servidores web de qualquer endereço IPv4.
0.0.0.0/0	TCP	443	Permite acesso HTTPS de entrada para servidores web de qualquer endereço IPv4
Intervalo de endereço IPv4 público da sua rede	TCP	22	(Instâncias Linux) Permite acesso SSH de entrada de sua rede por IPv4. Você pode obter o endereço IPv4 público de seu computador local usando um serviço como o http://checkip.amazonaws.com ou o https://checkip.amazonaws.com. Se estiver conectado por meio de um ISP ou atrás de um firewall sem um endereço IP estático, localize o intervalo de endereços IP usado por computadores cliente.
Intervalo de endereço IPv4 público da sua rede	TCP	3389	(Instâncias Windows) Permite acesso RDP de entrada de sua rede por IPv4.
O ID do security group (sg-xxxxxxxx)	Tudo	Tudo	(Opcional) Permite tráfego de entrada de outras instâncias associado a este security group. Esta regra é, automaticamente, adicionada ao security group padrão para a VPC;. Para qualquer security group personalizado que você criar, será preciso adicionar, manualmente, a regra que permite este tipo de comunicação.

Saída (Opcional)

Destino	Protocolo	Intervalo de portas	Comentários

0.0.0.0/0	Tudo	Tudo	Regra padrão para permitir todo acesso de saída a qualquer endereço IPv4. Se desejar que o servidor da web inicie o tráfego de saída, por exemplo, para adquirir atualizações de software, é possível manter a regra de saída padrão. Caso contrário, você não poderá remover essa regra.

Regras de grupos de segurança para IPv6

Se você associar um bloco CIDR IPv6 à sua VPC e à sub-rede, deverá adicionar regras distintas para seu security group, a fim de controlar o tráfego IPv6 de entrada e saída da instância do servidor da web. Neste cenário, o servidor da web poderá receber todo o tráfego da Internet por IPv6 e o tráfego RDP ou SSH da sua rede local por IPv6.

A seguir encontram-se regras específicas do IPv6 ao security group WebServerSG (que são um complemento às regras listadas anteriormente).

Entrada			
Origem	Protocolo	Intervalo de portas	Comentários
::/0	TCP	80	Permite acesso HTTP de entrada para servidores web de qualquer endereço IPv6.
::/0	TCP	443	Permite acesso HTTPS de entrada para servidores web de qualquer endereço IPv6.
Intervalo de endereços IPv6 de sua rede	TCP	22	(Instâncias Linux) Permite acesso SSH de entrada de sua rede por IPv6.
Intervalo de endereços IPv6 de sua rede	TCP	3389	(Instâncias Windows) Permite acesso RDP de entrada de sua rede por IPv6
Saída (Opcional)			
Destino	Protocolo	Intervalo de portas	Comentários
::/0	Tudo	Tudo	Regra padrão para permitir todo acesso de saída a qualquer endereço IPv6.

					Se desejar que o servidor da web inicie o tráfego de saída, por exemplo, para adquirir atualizações de software, é possível manter a regra de saída padrão. Caso contrário, você não poderá remover essa regra.

Regras de network ACL recomendadas para uma VPC com uma única sub-rede pública

A tabela a seguir mostra as regras que recomendamos. Elas bloqueiam todos os tráfegos, exceto aquele explicitamente necessário.

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	PERMISSÃO	Permite tráfego HTTP de entrada de qualquer endereço IPv4.
110	0.0.0.0/0	TCP	443	PERMISSÃO	Permite tráfego HTTPS de entrada de qualquer endereço IPv4.
120	Intervalo de endereços IPv4 públicos de sua rede doméstica	TCP	22	PERMISSÃO	Permite tráfego SSH de entrada de sua rede doméstica (pelo gateway da Internet).
130	Intervalo de endereços IPv4 públicos de sua rede doméstica	TCP	3389	PERMISSÃO	Permite tráfego RDP de entrada de sua rede doméstica (pelo gateway da Internet).
140	0.0.0.0/0	TCP	32768-65535	PERMISSÃO	Permite tráfego de retorno de entrada de hosts na Internet que estão respondendo a solicitações

					originadas na sub-rede. O intervalo é apenas de exemplo. Para obter informações sobre como escolher as portas efêmeras corretas para sua configuração, consulte Portas efêmeras (p. 202).
*	0.0.0.0/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos IPv4 de entrada ainda não controlados por uma regra precedente (não modificável).
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	PERMISSÃO	Permite tráfego HTTP de saída da sub-rede para a Internet.
110	0.0.0.0/0	TCP	443	PERMISSÃO	Permite tráfego HTTPS de saída da sub-rede para a Internet.

120	0.0.0.0/0	TCP	32768-65535	PERMISSÃO	Permite respostas de saída a clientes na Internet (por exemplo, fornece páginas da web a pessoas que visitam os servidores da web na sub-rede). O intervalo é apenas de exemplo. Para obter informações sobre como escolher as portas efêmeras corretas para sua configuração, consulte Portas efêmeras (p. 202).
*	0.0.0.0/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos IPv4 de saída ainda não controlados por uma regra precedente (não modificável).

Regras de network ACL recomendadas para IPv6

Se tiver implementado o suporte de IPv6 e criado uma VPC e uma sub-rede com blocos CIDR de IPv6 associados, deverá adicionar regras distintas à network ACL para controlar o tráfego IPv6 de entrada e saída.

Veja a seguir regras específicas de IPv6 para sua network ACL (que são um complemento às regras precedentes).

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
150	::/0	TCP	80	PERMISSÃO	Permite tráfego HTTP de entrada de qualquer endereço IPv6.

160	::/0	TCP	443	PERMISSÃO	Permite tráfego HTTPS de entrada de qualquer endereço IPv6.
170	Intervalo de endereços IPv6 de sua rede doméstica	TCP	22	PERMISSÃO	Permite tráfego SSH de entrada de sua rede doméstica (pelo gateway da Internet).
180	Intervalo de endereços IPv6 de sua rede doméstica	TCP	3389	PERMISSÃO	Permite tráfego RDP de entrada de sua rede doméstica (pelo gateway da Internet).
190	::/0	TCP	32768-65535	PERMISSÃO	Permite tráfego de retorno de entrada de hosts na Internet que estão respondendo a solicitações originadas na sub-rede. O intervalo é apenas de exemplo. Para obter informações sobre como escolher as portas efêmeras corretas para sua configuração, consulte Portas efêmeras (p. 202).
*	::/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos IPv6 de entrada ainda não controlados por uma regra precedente (não modificável).
Outbound					

Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
130	::/0	TCP	80	PERMISSÃO	Permite tráfego HTTP de saída da sub-rede para a Internet.
140	::/0	TCP	443	PERMISSÃO	Permite tráfego HTTPS de saída da sub-rede para a Internet.
150	::/0	TCP	32768-65535	PERMISSÃO	Permite respostas de saída a clientes na Internet (por exemplo, fornece páginas da web a pessoas que visitam os servidores da web na sub-rede). O intervalo é apenas de exemplo. Para obter informações sobre como escolher as portas efêmeras corretas para sua configuração, consulte Portas efêmeras (p. 202).
*	::/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos IPv6 de saída ainda não controlados por uma regra precedente (não modificável).

VPC com sub-redes públicas e privadas (NAT)

A configuração desse cenário inclui uma virtual private cloud (VPC) com uma sub-rede pública e uma sub-rede privada. Recomendamos este cenário se você quiser executar um aplicativo web voltado para o público e ao mesmo tempo manter servidores back-end sem acesso público. Um exemplo comum é um

site de várias camadas, com servidores web em uma sub-rede pública e servidores de banco de dados em uma sub-rede privada. Você pode configurar segurança e roteamento para que os servidores web comuniquem-se com os servidores de banco de dados.

As instâncias na sub-rede pública podem enviar tráfego de saída diretamente para a Internet, ao passo que as instâncias na sub-rede privada não podem. Em vez disso, as instâncias da sub-rede privada podem acessar a Internet usando um gateway de conversão de endereços de rede (NAT) que resida na sub-rede pública. Os servidores de banco de dados podem se conectar à Internet para atualizações de software usando gateway NAT, mas a Internet não pode estabelecer conexões com os servidores de banco de dados.

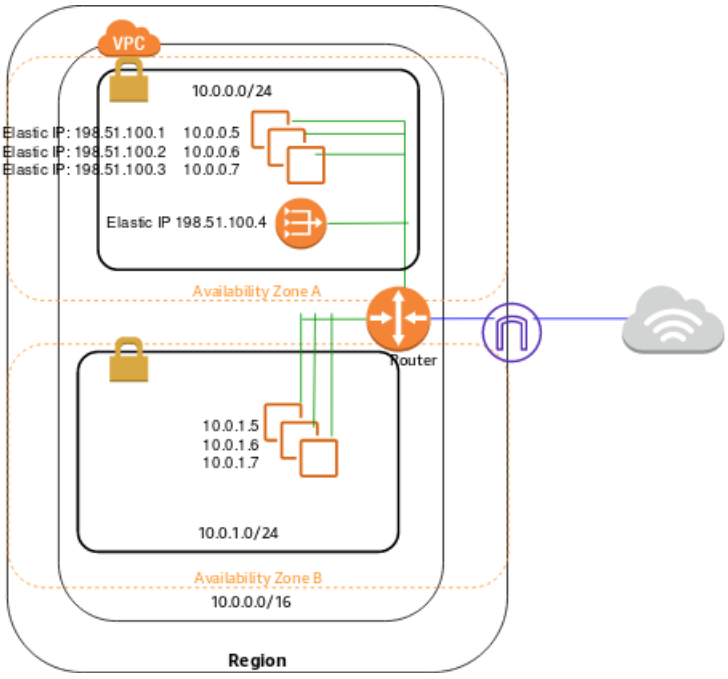
Além disso, este cenário pode ser opcionalmente configurado para IPv6: é possível usar o assistente de VPC para criar uma VPC e sub-redes com blocos CIDR IPv6 associados. as instâncias executadas em sub-redes podem receber endereços IPv6 e se comunicar usando IPv6. As instâncias na sub-rede privada podem usar um gateway da Internet apenas de saída para se conectar à Internet por IPv6, mas a Internet não pode estabelecer conexões com as instâncias privadas por IPv6. Para obter mais informações sobre endereçamento IPv4 e IPv6, consulte Endereçamento IP na sua VPC (p. 117).

Para obter informações sobre como gerenciar o software de instância do EC2, consulte Gerenciar software na instância do Linux no Guia do usuário do Amazon EC2 para instâncias do Linux.

Tópicos

Visão geral

O diagrama a seguir mostra os principais componentes da configuração deste cenário.



A configuração deste cenário inclui o seguinte:

- VPC com bloco CIDR IPv4 tamanho /16 (exemplo: 10.0.0.0/16). Nesse caso, são fornecidos 65.536 endereços IPv4.
- Sub-rede pública com bloco CIDR IPv4 tamanho /24 (exemplo: 10.0.0.0/24). Nesse caso, são fornecidos 256 endereços IPv4. A sub-rede pública é uma sub-rede associada a uma tabela de rotas que contém uma rota para um gateway da Internet.
- Sub-rede privada com bloco CIDR IPv4 tamanho /24 (exemplo: 10.0.1.0/24). Nesse caso, são fornecidos 256 endereços IPv4.
- Um gateway de internet. Isso conecta a VPC à Internet e a outros serviços da AWS.
- Instâncias com endereços IPv4 privados no intervalo da sub-rede (exemplos: 10.0.0.5, 10.0.1.5). Isso permite que elas se comuniquem entre si e com outras instâncias na VPC.
- Instâncias na sub-rede pública com endereços IPv4 elásticos (exemplo: 198.51.100.1), os quais são endereços IPv4 públicos que permitem que elas sejam acessadas pela Internet. Instâncias que têm endereços IP públicos atribuídos na execução, em vez de endereços IP elásticos. As instâncias na sub-rede privada são servidores back-end que não precisam aceitar tráfego de entrada da Internet e por isso não têm endereços IP públicos; entretanto, elas podem enviar solicitações para a Internet usando o gateway NAT (consulte o próximo item).
- Gateway NAT com seu próprio endereço IPv4 elástico. As instâncias na sub-rede privada podem enviar solicitações para a Internet por meio do gateway NAT por IPv4 (por exemplo, para atualizações de software).
- Uma tabela de rotas personalizada associada à sub-rede pública. Essa tabela de rotas contém uma entrada que permite que as instâncias da sub-rede comuniquem-se com outras instâncias na VPC por IPv4 e uma entrada que permite que as instâncias da sub-rede comuniquem-se diretamente com a Internet por IPv4.
- Tabela de rotas principal associada à sub-rede privada. Essa tabela de rotas contém uma entrada que permite que as instâncias da sub-rede comuniquem-se com outras instâncias na VPC por IPv4 e uma entrada que permite que as instâncias da sub-rede comuniquem-se diretamente com a Internet por meio do gateway NAT e por IPv4.

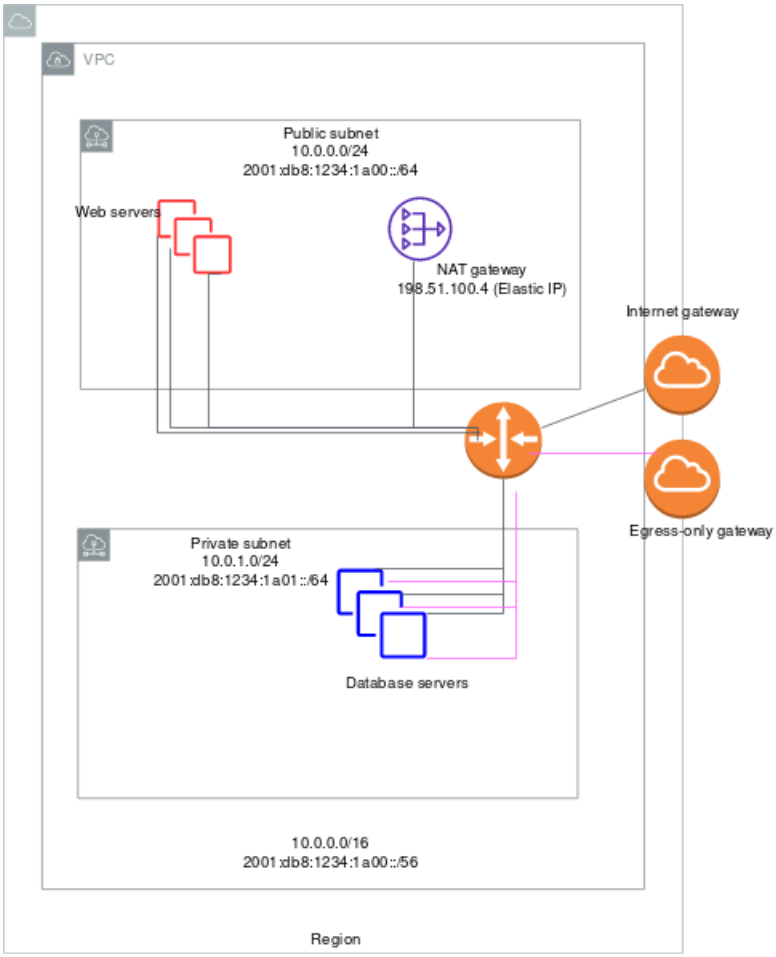
Para obter mais informações sobre sub-redes, consulte VPCs e sub-redes (p. 100). Para obter mais informações sobre gateways da Internet, consulte Gateways da Internet (p. 212). Para obter mais informações sobre gateways NAT;, consulte Gateways NAT (p. 229).

Visão geral de IPv6

Opcionalmente, você pode ativar o IPv6 para este cenário. Além dos componentes listados anteriormente, a configuração inclui o seguinte:

- Um bloco CIDR IPv6 tamanho /56 associado à VPC (exemplo: 2001:db8:1234:1a00::/56). A Amazon atribui automaticamente o CIDR; você não pode escolher o intervalo.
- Um bloco CIDR IPv6 tamanho /64 associado a uma sub-rede pública (exemplo: 2001:db8:1234:1a00::/64). Você pode escolher o intervalo para sua sub-rede com base no intervalo alocado à VPC. Você não pode escolher o tamanho do bloco CIDR IPv6 da VPC.
- Bloco CIDR IPv6 tamanho /64 associado a uma sub-rede privada (exemplo: 2001:db8:1234:1a01::/64). Você pode escolher o intervalo para sua sub-rede com base no intervalo alocado à VPC. Você não pode escolher o tamanho do bloco CIDR IPv6 da sub-rede.
- Endereços IPv6 atribuídos às instâncias no intervalo da sub-rede (exemplo: 2001:db8:1234:1a00::1a).
- Um gateway da Internet apenas de saída. Você usa o gateway para lidar com solicitações para a Internet de instâncias na sub-rede privada por IPv6 (por exemplo, para atualizações de software). Será necessário usar um gateway da Internet apenas de saída se desejar que as instâncias na sub-rede privada estabeleçam comunicação com a Internet por IPv6. Para obter mais informações, consulte Gateways da Internet apenas de saída (p. 218).

- Entradas na tabela de rotas personalizada que permitem que as instâncias na sub-rede pública usem IPv6 para se comunicarem entre si e diretamente na Internet.
- Entradas de rotas na tabela de rotas principal que permite que as instâncias na sub-rede privada usem IPv6 para se comunicar entre si e para se comunicar com a Internet por meio de gateway da Internet apenas de saída.



Os servidores web na sub-rede pública têm os endereços a seguir.

de aplicativos	IPv4 address (Endereço IPv4)	Endereços elastic IP (EIPs)	Endereço IPv6
1	10.0.0.5	198.51.100.1	2001:db8:1234:1a00::1a
2	10.0.0.6	198.51.100.2	2001:db8:1234:1a00::2b
3	10.0.0.7	198.51.100.3	2001:db8:1234:1a00::3c

Os servidores de banco de dados na sub-rede privada têm os endereços a seguir.

de aplicativos	IPv4 address (Endereço IPv4)	Endereço IPv6
1	10.0.1.5	2001:db8:1234:1a01::1a
2	10.0.1.6	2001:db8:1234:1a01::2b
3	10.0.1.7	2001:db8:1234:1a01::3c

Roteamento

Neste cenário, o assistente de VPC atualiza a tabela de rotas principal usada na sub-rede privada e cria uma tabela de rotas personalizada e a associa à sub-rede pública.

Nesse cenário, todos os tráfegos provenientes de cada sub-rede vinculada à AWS (por exemplo, aos endpoints do Amazon EC2 ou do Amazon S3) passam pelo gateway da Internet. Os servidores de banco de dados na sub-rede privada não podem receber tráfego diretamente da Internet porque eles não têm endereços IP elásticos. Entretanto, os servidores de banco de dados podem enviar e receber tráfego da Internet por meio do dispositivo NAT na sub-rede pública.

Quaisquer outras sub-redes que você criar usarão a tabela de rotas principal por padrão, o que significa que elas são sub-redes privadas por padrão. Quando desejar tornar uma sub-rede pública, sempre é possível alterar a tabela de rotas principal com a qual está associada.

As tabelas a seguir descrevem as tabelas de rotas para este cenário.

Tabela de rotas principal

Tabela de rotas principal associada à sub-rede privada. A primeira entrada é a padrão para roteamento local na VPC; essa entrada permite que as instâncias na VPC comuniquem-se entre si. A segunda entrada envia todos os outros tráfegos da sub-rede ao gateway NAT (por exemplo, `nat-1234567890123456`7).

Destino	Destino
`10.0.0.0/16`	local
`0.0.0.0/0`	nat-gateway-id

Tabela de rotas personalizada

Uma tabela de rotas personalizada é associada à sub-rede pública. A primeira entrada é a padrão para um roteamento local na VPC; essa entrada permite que as instâncias na VPC comuniquem-se entre si. A segunda entrada roteia todos os outros tráfegos da sub-rede à Internet por meio do gateway da Internet (por exemplo, `igw-1a2b3d4d`).

Destino	Destino
`10.0.0.0/16`	local
`0.0.0.0/0`	igw-id

Roteamento para o IPv6

Se você associar um bloco CIDR IPv6 à sua VPC e às sub-redes, a tabela de rotas deverá incluir rotas distintas para tráfego IPv6. As tabelas a seguir mostram a tabela de rotas personalizada para este cenário, se você escolher permitir comunicação IPv6 em sua VPC.

Tabela de rotas principal

A segunda entrada é a rota padrão adicionada automaticamente para roteamento local na VPC via IPv6. A quarta entrada roteia todos os outros tráfegos IPv6 da sub-rede para o gateway da Internet apenas de saída.

Destino	Destino
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
0.0.0.0/0	nat-gateway-id
::/0	egress-only-igw-id

Tabela de rotas personalizada

A segunda entrada é a rota padrão adicionada automaticamente para roteamento local na VPC via IPv6. A quarta entrada roteia todos os outros tráfegos IPv6 da sub-rede para o gateway da Internet.

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

A AWS fornece dois recursos que você pode usar para aumentar a segurança da VPC: grupos de segurança e ACLs da rede. Os grupos de segurança controlam o tráfego de entrada e de saída de suas instâncias e as Network ACL controlam o tráfego de entrada e de saída de suas sub-redes. Na maioria dos casos, os grupos de segurança podem atender as suas necessidades; contudo, você também pode usar as Network ACL se desejar uma camada adicional de segurança para o seu VPC. Para obter mais informações, consulte Privacidade do tráfego entre redes na Amazon VPC (p. 158).

No cenário 2, você usará security groups, mas não Network ACLs. Se quiser usar uma network ACL, consulte Regras de network ACL recomendadas para uma VPC com sub-redes públicas e privadas (NAT) (p. 40).

Sua VPC é fornecida com um security group padrão (p. 181). Uma instância executada na VPC será automaticamente associada ao security group padrão se você não especificar um security group diferente durante a execução. Para este cenário, é recomendável criar os security groups a seguir, em vez de usar o security group padrão:

- WebServerSG: especifique esse security group quando iniciar servidores web na sub-rede pública.
- DBServerSG: especifique esse security group quando iniciar os servidores de banco de dados na sub-rede privada.

As instâncias atribuídas a um security group podem estar em diferentes sub-redes. Entretanto, neste cenário, cada security group corresponde ao tipo de função que uma instância desempenha e cada função

requer que a instância esteja em uma sub-rede específica. Portanto, neste cenário, todas as instâncias atribuídas a um security group estão na mesma sub-rede.

A tabela a seguir descreve as regras recomendadas para o grupo de segurança WebServerSG, que permitem que os servidores web recebam tráfego da Internet, bem como tráfego SSH e RDP de sua rede. Os servidores web podem também iniciar solicitações de leitura e gravação para os servidores de banco de dados na sub-rede privada e enviar tráfego para a Internet; por exemplo, para obter atualizações de software. Pelo fato de o servidor Web não iniciar nenhuma outra comunicação de saída, a regra de saída padrão é removida.

> **Note**
>
> Essas recomendações incluem o acesso SSH e RDP e acesso do Microsoft SQL Server e MySQL. Na sua situação, talvez você precise apenas de regras para o Linux (SSH e MySQL) ou Windows (RDP e Microsoft SQL Server).

WebServerSG: regras recomendadas

Entrada			
Origem	Protocolo	Intervalo de portas	Comentários
0.0.0.0/0	TCP	80	Permite acesso HTTP de entrada para servidores web de qualquer endereço IPv4.
0.0.0.0/0	TCP	443	Permite acesso HTTPS de entrada para servidores web de qualquer endereço IPv4.
Intervalo de endereços IPv4 públicos de sua rede doméstica	TCP	22	Permite acesso SSH de entrada de sua rede doméstica a instâncias Linux (por meio do gateway da Internet). Você pode obter o endereço IPv4 público de seu computador local usando um serviço como o http://checkip.amazonaws.com ou o https://checkip.amazonaws.com. Se estiver conectado por meio de um ISP ou atrás de um firewall sem um endereço IP estático, localize o intervalo de endereços IP usado por computadores cliente.
Intervalo de endereços IPv4 públicos de sua rede doméstica	TCP	3389	Permite acesso RDP de entrada de sua rede doméstica a instâncias Windows (por meio do gateway da Internet).

Saída			
Destino	Protocolo	Intervalo de portas	Comentários
ID do security group DBServerSG	TCP	1433	Permite acesso de saída do Microsoft SQL Server aos servidores de banco de dados atribuídos ao security group DBServerSG.
ID do security group DBServerSG	TCP	3306	Permite acesso de saída do MySQL aos servidores de banco de dados atribuídos ao security group DBServerSG.
0.0.0.0/0	TCP	80	Permite acesso HTTP de saída a qualquer endereço IPv4.
0.0.0.0/0	TCP	443	Permite acesso HTTPS de saída a qualquer endereço IPv4.

A tabela a seguir descreve as regras recomendadas para o security group DBServerSG, que permitem solicitações de leitura e gravação ao banco de dados nos servidores web. Os servidores de banco de dados podem também iniciar tráfego destinado à Internet (a tabela de rotas envia o tráfego ao gateway NAT, que o encaminha à Internet por meio do gateway da Internet).

DBServerSG: regras recomendadas

Entrada			
Origem	Protocolo	Intervalo de portas	Comentários
ID do security group WebServerSG	TCP	1433	Permite acesso de entrada ao Microsoft SQL Server de servidores web associados ao security group WebServerSG.
ID do security group WebServerSG	TCP	3306	Permite acesso de entrada ao MySQL Server de servidores web associados ao security group WebServerSG.
Saída			
Destino	Protocolo	Intervalo de portas	Comentários
0.0.0.0/0	TCP	80	Permite acesso HTTP de saída à Internet por IPv4 (por exemplo,

			para atualizações de software).
0.0.0.0/0	TCP	443	Permite acesso HTTPS de saída à Internet por IPv4 (por exemplo, para atualizações de software).

(Opcional) O security group padrão para uma VPC tem regras que permite automaticamente que as instâncias atribuídas comuniquem-se entre si. Para permitir esse tipo de comunicação a um security group personalizado, é necessário adicionar as regras a seguir:

Entrada			
Origem	Protocolo	Intervalo de portas	Comentários
ID do security group	Tudo	Tudo	(Opcional) Permite tráfego de entrada de outras instâncias atribuídas para esse security group.
Saída			
Destino	Protocolo	Intervalo de portas	Comentários
ID do security group	Tudo	Tudo	Permite tráfego de saída a outras instâncias atribuídas para esse security group.

(Opcional) Se você executar um bastion host na sub-rede pública para ser usado como proxy para tráfego SSH ou RDP da rede doméstica à sub-rede privada, adicione uma regra ao security group DBServerSG que permita que o tráfego de entrada SSH ou RDP da instância do bastion ou do seu security group associado.

Regras de grupos de segurança para IPv6

Se você associar um bloco CIDR IPv6 à sua VPC e às sub-redes, deverá adicionar regras distintas aos seus security groups WebServerSG e DBServerSG a fim de controlar o tráfego IPv6 de entrada e saída de suas instâncias. Neste cenário, os servidores web poderão receber todo o tráfego da Internet por IPv6 e tráfego RDP ou SSH de sua rede local por IPv6. Além disso, eles poderão iniciar tráfego IPv6 de saída para a Internet. Os servidores de banco de dados podem iniciar tráfego IPv6 de saída para a Internet.

A seguir encontram-se regras específicas do IPv6 ao security group WebServerSG (que são um complemento às regras listadas anteriormente).

Entrada			
Origem	Protocolo	Intervalo de portas	Comentários
::/0	TCP	80	Permite acesso HTTP de entrada para servidores web de qualquer endereço IPv6.

::/0	TCP	443	Permite acesso HTTPS de entrada para servidores web de qualquer endereço IPv6.
Intervalo de endereços IPv6 de sua rede	TCP	22	(Instâncias Linux) Permite acesso SSH de entrada de sua rede por IPv6.
Intervalo de endereços IPv6 de sua rede	TCP	3389	(Instâncias Windows) Permite acesso RDP de entrada de sua rede por IPv6
Saída			
Destino	Protocolo	Intervalo de portas	Comentários
::/0	TCP	HTTP	Permite acesso HTTP de saída a qualquer endereço IPv6.
::/0	TCP	HTTPS	Permite acesso HTTPS de saída a qualquer endereço IPv6.

A seguir encontram-se regras específicas do IPv6 ao security group DBServerSG (que são um complemento às regras listadas anteriormente).

Saída			
Destino	Protocolo	Intervalo de portas	Comentários
::/0	TCP	80	Permite acesso HTTP de saída a qualquer endereço IPv6.
::/0	TCP	443	Permite acesso HTTPS de saída a qualquer endereço IPv6.

Implementar o cenário 2

Você pode usar o assistente de VPC para criar a VPC, sub-redes, gateway NAT e, opcionalmente, um gateway da Internet apenas de saída. Você precisa especificar um endereço IP elástico para seu gateway NAT; se não tiver um, primeiro deverá alocar um à sua conta. Se desejar usar um endereço IP elástico existente, verifique se no momento ele não está associado a outra instância ou interface de rede. O gateway NAT é criado automaticamente na sub-rede pública de sua VPC.

Regras de network ACL recomendadas para uma VPC com sub-redes públicas e privadas (NAT)

Para esse cenário você tem uma network ACL para a sub-rede pública e outra network ACL para a sub-rede privada. A tabela a seguir mostra as regras que recomendamos para cada ACL. Elas bloqueiam todos

os tráfegos, exceto aquele explicitamente necessário. Eles basicamente imitam as regras do security group do cenário.

Regras de ACL para sub-rede pública

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	PERMISSÃO	Permite tráfego HTTP de entrada de qualquer endereço IPv4.
110	0.0.0.0/0	TCP	443	PERMISSÃO	Permite tráfego HTTPS de entrada de qualquer endereço IPv4.
120	Intervalo de endereços IP públicos da sua rede doméstica	TCP	22	PERMISSÃO	Permite tráfego SSH de entrada de sua rede doméstica (pelo gateway da Internet).
130	Intervalo de endereços IP públicos da sua rede doméstica	TCP	3389	PERMISSÃO	Permite tráfego RDP de entrada de sua rede doméstica (pelo gateway da Internet).
140	0.0.0.0/0	TCP	1024-65535	PERMISSÃO	Permite tráfego de retorno de entrada de hosts na Internet que estão respondendo a solicitações originadas na sub-rede. O intervalo é apenas de exemplo. Para obter informações sobre como escolher as portas efêmeras corretas para sua configuração,

					consulte Portas efêmeras (p. 202).
*	0.0.0.0/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos IPv4 de entrada ainda não controlados por uma regra precedente (não modificável).
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	PERMISSÃO	Permite tráfego HTTP de saída da sub-rede para a Internet.
110	0.0.0.0/0	TCP	443	PERMISSÃO	Permite tráfego HTTPS de saída da sub-rede para a Internet.
120	10.0.1.0/24	TCP	1433	PERMISSÃO	Permite acesso MS SQL de saída a servidores de banco de dados na sub-rede privada. Esse número de porta é apenas de exemplo. Outros exemplos incluem 3306 para acesso MySQL/ Aurora, 5432 para acesso PostgreSQL, 5439 para acesso Amazon Redshift e 1521 para acesso Oracle.

140	0.0.0.0/0	TCP	32768-65535	PERMISSÃO	Permite respostas de saída a clientes na Internet (por exemplo, fornece páginas da web a pessoas que visitam os servidores da web na sub-rede). O intervalo é apenas de exemplo. Para obter informações sobre como escolher as portas efêmeras corretas para sua configuração, consulte Portas efêmeras (p. 202).
150	10.0.1.0/24	TCP	22	PERMISSÃO	Permite acesso SSH de saída a instância em sua sub-rede privada (de um SSH Bastion, se tiver um).
*	0.0.0.0/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos IPv4 de saída ainda não controlados por uma regra precedente (não modificável).

Regras de ACL para sub-rede privada

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
100	10.0.0.0/24	TCP	1433	PERMISSÃO	Permite que servidores web na sub-rede pública leiam e gravem em

					servidores MS SQL na sub-rede privada. Esse número de porta é apenas de exemplo. Outros exemplos incluem 3306 para acesso MySQL/ Aurora, 5432 para acesso PostgreSQL, 5439 para acesso Amazon Redshift e 1521 para acesso Oracle.
120	10.0.0.0/24	TCP	22	PERMISSÃO	Permite tráfego SSH de entrada de um SSH Bastion na sub-rede pública (se tiver um).
130	10.0.0.0/24	TCP	3389	PERMISSÃO	Permite tráfego RDP de entrada do gateway Microsoft Terminal Services na sub-rede pública.

140	0.0.0.0/0	TCP	1024-65535	PERMISSÃO	Permite tráfego de retorno de saída do dispositivo NAT na sub-rede pública para solicitações originadas na sub-rede privada. Para obter informações sobre como especificar as portas efêmeras corretas, consulte uma observação fundamental no início deste tópico.
*	0.0.0.0/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos IPv4 de entrada ainda não controlados por uma regra precedente (não modificável).

Outbound

Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	PERMISSÃO	Permite tráfego HTTP de saída da sub-rede para a Internet.
110	0.0.0.0/0	TCP	443	PERMISSÃO	Permite tráfego HTTPS de saída da sub-rede para a Internet.

120	10.0.0.0/24	TCP	32768-65535	PERMISSÃO	Permite respostas de saída à sub-rede pública (por exemplo, respostas de servidores web na sub-rede pública que estão se comunicando com servidores de banco de dados na sub-rede privada). O intervalo é apenas de exemplo. Para obter informações sobre como escolher as portas efêmeras corretas para sua configuração, consulte Portas efêmeras (p. 202).
*	0.0.0.0/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos IPv4 de saída ainda não controlados por uma regra precedente (não modificável).

Regras de network ACL recomendadas para IPv6

Se tiver implementado suporte de IPv6 e criado uma VPC e sub-redes com blocos CIDR de IPv6 associados, deverá adicionar regras distintas às suas network ACLs para controlar o tráfego IPv6 de entrada e saída.

Veja a seguir regras específicas de IPv6 para suas network ACLs (que são um complemento às regras precedentes).

Regras de ACL para sub-rede pública

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments

150	::/0	TCP	80	PERMISSÃO	Permite tráfego HTTP de entrada de qualquer endereço IPv6.
160	::/0	TCP	443	PERMISSÃO	Permite tráfego HTTPS de entrada de qualquer endereço IPv6.
170	Intervalo de endereços IPv6 de sua rede doméstica	TCP	22	PERMISSÃO	Permite tráfego SSH de entrada por IPv6 de sua rede doméstica (pelo gateway da Internet).
180	Intervalo de endereços IPv6 de sua rede doméstica	TCP	3389	PERMISSÃO	Permite tráfego RDP de entrada por IPv6 de sua rede doméstica (pelo gateway da Internet).
190	::/0	TCP	1024-65535	PERMISSÃO	Permite tráfego de retorno de entrada de hosts na Internet que estão respondendo a solicitações originadas na sub-rede. O intervalo é apenas de exemplo. Para obter informações sobre como escolher as portas efêmeras corretas para sua configuração, consulte Portas efêmeras (p. 202).

*	::/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos IPv6 de entrada ainda não controlados por uma regra precedente (não modificável).
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
160	::/0	TCP	80	PERMISSÃO	Permite tráfego HTTP de saída da sub-rede para a Internet.
170	::/0	TCP	443	PERMISSÃO	Permite tráfego HTTPS de saída da sub-rede para a Internet
180	2001:db8:1234:1a00::/64	TCP	1433	PERMISSÃO	Permite acesso MS SQL de saída a servidores de banco de dados na sub-rede privada. Esse número de porta é apenas de exemplo. Outros exemplos incluem 3306 para acesso MySQL/ Aurora, 5432 para acesso PostgreSQL, 5439 para acesso Amazon Redshift e 1521 para acesso Oracle.

200	::/0	TCP	32768-65535	PERMISSÃO	Permite respostas de saída a clientes na Internet (por exemplo, fornece páginas da web a pessoas que visitam os servidores da web na sub-rede). O intervalo é apenas de exemplo. Para obter informações sobre como escolher as portas efêmeras corretas para sua configuração, consulte Portas efêmeras (p. 202).
210	2001:db8:1234:1a00::/64	TCP	22	PERMISSÃO	Permite acesso SSH de saída a instância em sua sub-rede privada (de um SSH Bastion, se tiver um).
*	::/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos IPv6 de saída ainda não controlados por uma regra precedente (não modificável).

Regras de ACL para sub-rede privada

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
150	2001:db8:1234:1a00::/64	TCP	1433	PERMISSÃO	Permite que servidores web na sub-rede pública leiam e gravem em

					servidores MS SQL na sub-rede privada. Esse número de porta é apenas de exemplo. Outros exemplos incluem 3306 para acesso MySQL/ Aurora, 5432 para acesso PostgreSQL, 5439 para acesso Amazon Redshift e 1521 para acesso Oracle.
170	2001:db8:1234:1a00::/64	TCP	22	PERMISSÃO	Permite tráfego SSH de entrada de um SSH Bastion na sub-rede pública (se aplicável).
180	2001:db8:1234:1a00::/64	TCP	3389	PERMISSÃO	Permite tráfego RDP de entrada de um gateway Microsoft Terminal Services na sub-rede pública, se aplicável.

190	::/0	TCP	1024-65535	PERMISSÃO	Permite tráfego de retorno de entrada do gateway da Internet apenas de saída para solicitações originadas na sub-rede privada. O intervalo é apenas de exemplo. Para obter informações sobre como escolher as portas efêmeras corretas para sua configuração, consulte Portas efêmeras (p. 202).
*	::/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos IPv6 de entrada ainda não controlados por uma regra precedente (não modificável).
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
130	::/0	TCP	80	PERMISSÃO	Permite tráfego HTTP de saída da sub-rede para a Internet.
140	::/0	TCP	443	PERMISSÃO	Permite tráfego HTTPS de saída da sub-rede para a Internet.

150	2001:db8:1234:1a00::/64	TCP	32768-65535	PERMISSÃO	Permite respostas de saída à sub-rede pública (por exemplo, respostas de servidores web na sub-rede pública que estão se comunicando com servidores de banco de dados na sub-rede privada). O intervalo é apenas de exemplo. Para obter informações sobre como escolher as portas efêmeras corretas para sua configuração, consulte Portas efêmeras (p. 202).
*	::/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos IPv6 de saída ainda não controlados por uma regra precedente (não modificável).

VPC com sub-redes públicas e privadas e acesso à AWS Site-to-Site VPN

A configuração deste cenário inclui uma virtual private cloud (VPC) com uma sub-rede pública e uma sub-rede privada e um gateway privado virtual para permitir comunicação com sua rede em um túnel VPN IPsec. Recomendamos este cenário se você quiser expandir sua rede para a nuvem e também acessar diretamente a Internet em sua VPC. Este cenário permite que você execute uma aplicação multicamadas com um front-end da Web escalável em uma sub-rede pública e armazene os dados em uma sub-rede privada que se conecta à rede por meio de uma conexão AWS Site-to-Site VPN de IPsec.

Além disso, este cenário pode ser opcionalmente configurado para IPv6: é possível usar o assistente de VPC para criar uma VPC e sub-redes com blocos CIDR IPv6 associados. As instâncias executadas nas sub-redes podem receber endereços IPv6. No momento, não oferecemos suporte à comunicação via IPv6 por meio de uma conexão Site-to-Site VPN em um gateway privado virtual. No entanto, as instâncias na

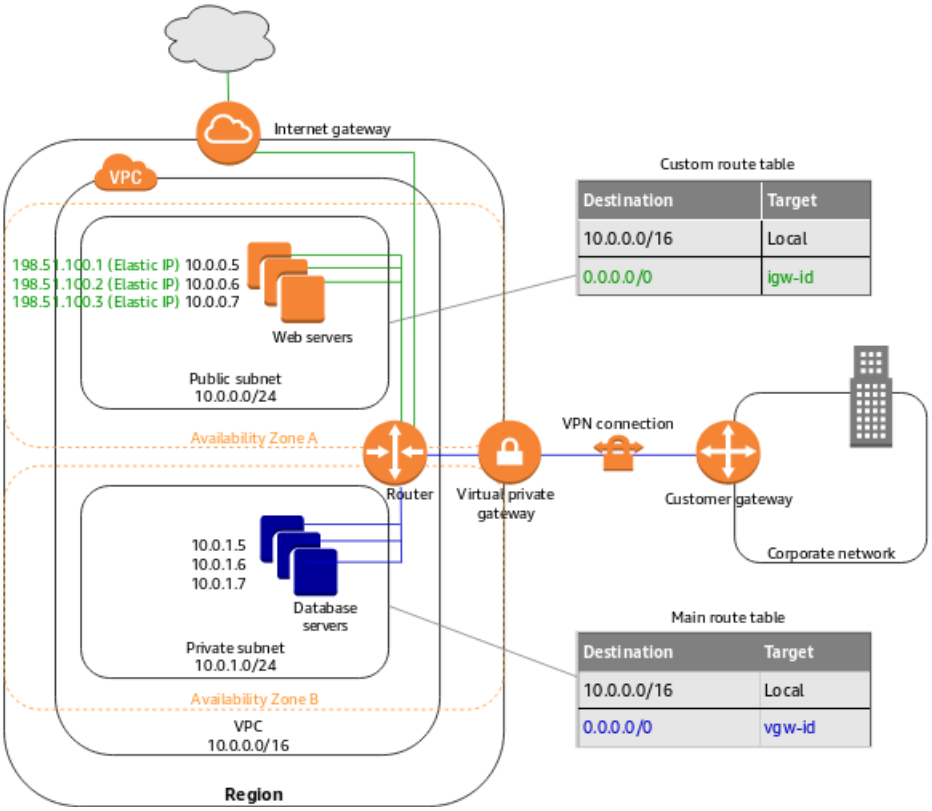
VPC podem se comunicar entre si via IPv6 e as instâncias na sub-rede pública podem se comunicar na Internet via IPv6. Para obter mais informações sobre endereçamento IPv4 e IPv6, consulte Endereçamento IP na sua VPC (p. 117).

Para obter informações sobre como gerenciar o software de instância do EC2, consulte Gerenciar software na instância do Linux no Guia do usuário do Amazon EC2 para instâncias do Linux.

Tópicos

Visão geral

O diagrama a seguir mostra os principais componentes da configuração deste cenário.



Important

Para esse cenário, consulte O dispositivo de gateway do cliente no Guia do usuário do AWS Site-to-Site VPN para obter informações sobre como configurar o dispositivo de gateway do cliente no seu lado da conexão do Site-to-Site VPN.

A configuração deste cenário inclui o seguinte:

- Uma virtual private cloud (VPC) com CIDR IPv4 tamanho /16 (exemplo: 10.0.0.0/16). Nesse caso, são fornecidos 65.536 endereços IPv4.

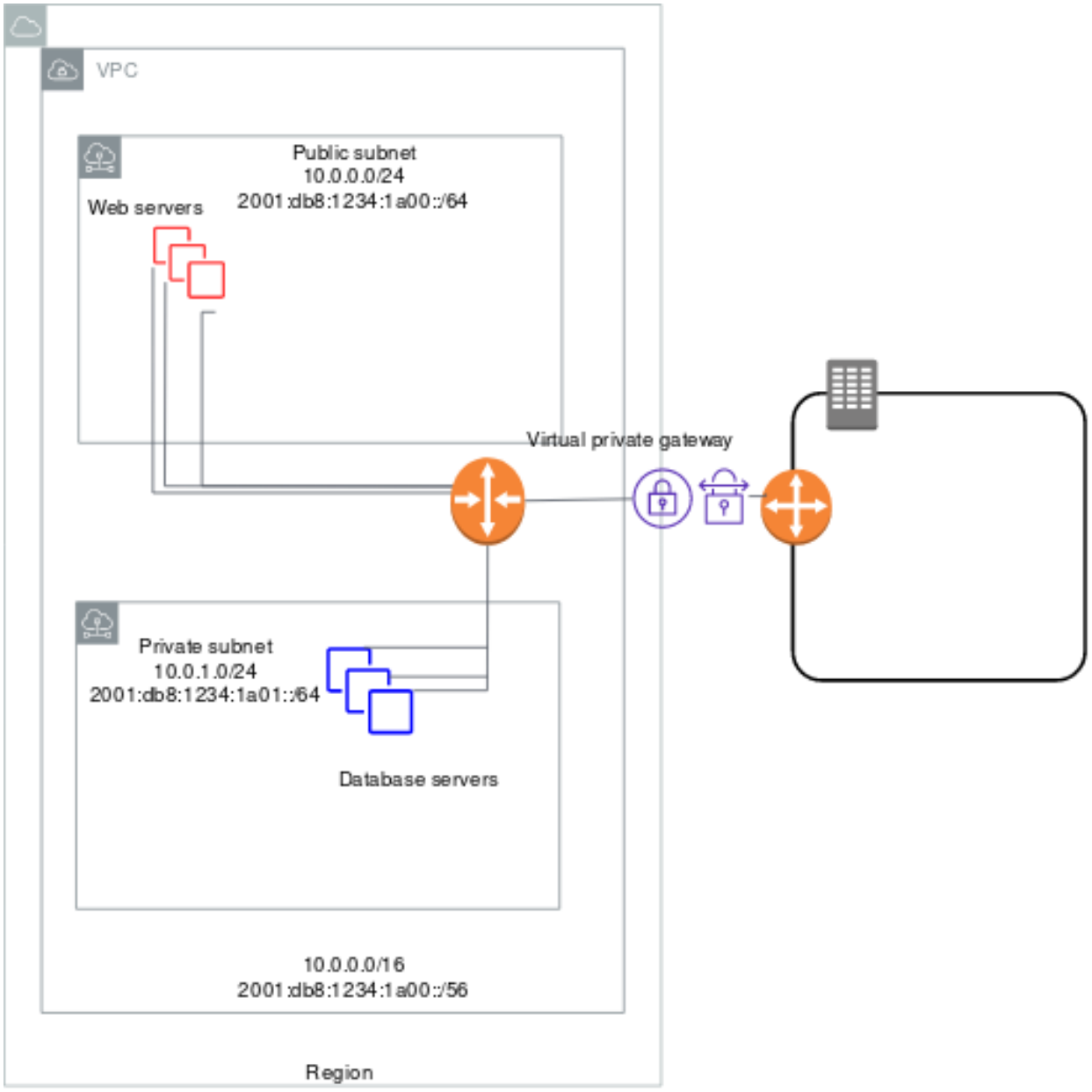
- Sub-rede pública com CIDR IPv4 tamanho /24 (exemplo: 10.0.0.0/24). Nesse caso, são fornecidos 256 endereços IPv4. A sub-rede pública é uma sub-rede associada a uma tabela de rotas que contém uma rota para um gateway da Internet.
- Sub-rede somente VPN com CIDR IPv4 tamanho /24 (exemplo: 10.0.1.0/24). Nesse caso, são fornecidos 256 endereços IPv4.
- Um gateway de internet. Desse modo a VPC é conectada à Internet e a outros produtos da AWS.
- Conexão Site-to-Site VPN entre a VPC e a rede. A conexão Site-to-Site VPN compreende um gateway privado virtual localizado na conexão Site-to-Site VPN do lado da Amazon e um gateway do cliente localizado na conexão Site-to-Site VPN do seu lado.
- As instâncias com endereços IPv4 privados no intervalo da sub-rede (exemplos: 10.0.0.5 e 10.0.1.5). Isso permite que as instâncias se comuniquem entre si e com outras instâncias na VPC.
- Instâncias na sub-rede pública com endereços IP elásticos (exemplo: 198.51.100.1), os quais são endereços IPv4 públicos que permitem que elas sejam acessadas pela Internet. Instâncias que têm endereços IPv4 públicos atribuídos na execução, em vez de endereços IP elásticos. As instâncias na sub-rede somente VPN são servidores back-end que não precisam aceitar tráfego de entrada da Internet, mas podem enviar e receber tráfego de sua rede.
- Uma tabela de rotas personalizada associada à sub-rede pública. Essa tabela de rotas contém uma entrada que permite que as instâncias da sub-rede comuniquem-se com outras instâncias na VPC e uma entrada que permite que as instâncias da sub-rede comuniquem-se diretamente com a Internet.
- Tabela de rotas principal associada à sub-rede somente VPN. A tabela de rotas contém uma entrada que permite que as instâncias da sub-rede comuniquem-se com outras instâncias na VPC e uma entrada que permite que as instâncias da sub-rede comuniquem-se diretamente com sua rede.

Para obter mais informações sobre sub-redes, consulte VPCs e sub-redes (p. 100) e Endereçamento IP na sua VPC (p. 117). Para obter mais informações sobre gateways da Internet, consulte Gateways da Internet (p. 212). Para obter mais informações sobre a conexão AWS Site-to-Site VPN, consulte O que é a AWS Site-to-Site VPN? no Guia do usuário da AWS Site-to-Site VPN.

Visão geral de IPv6

Opcionalmente, você pode ativar o IPv6 para este cenário. Além dos componentes listados anteriormente, a configuração inclui o seguinte:

- Um bloco CIDR IPv6 tamanho /56 associado à VPC (exemplo: 2001:db8:1234:1a00::/56). A AWS atribui automaticamente o CIDR; não é possível escolher o intervalo.
- Um bloco CIDR IPv6 tamanho /64 associado a uma sub-rede pública (exemplo: 2001:db8:1234:1a00::/64). Você pode escolher o intervalo para sua sub-rede com base no intervalo alocado à VPC. Você não pode escolher o tamanho do CIDR IPv6.
- Um bloco CIDR IPv6 tamanho /64 associado a uma sub-rede somente VPN (exemplo: 2001:db8:1234:1a01::/64). Você pode escolher o intervalo para sua sub-rede com base no intervalo alocado à VPC. Você não pode escolher o tamanho do CIDR IPv6.
- Endereços IPv6 atribuídos às instâncias no intervalo da sub-rede (exemplo: 2001:db8:1234:1a00::1a).
- Entradas na tabela de rotas personalizada que permitem que as instâncias na sub-rede pública usem IPv6 para se comunicarem entre si e diretamente na Internet.
- Uma entrada da tabela de rotas principal que permite que as instâncias na sub-rede somente VPN usem IPv6 para se comunicarem entre si.



Os servidores web na sub-rede pública têm os endereços a seguir.

de aplicativos	IPv4 address (Endereço IPv4)	Endereços elastic IP (EIPs)	Endereço IPv6
1	10.0.0.5	198.51.100.1	2001:db8:1234:1a00::1a
2	10.0.0.6	198.51.100.2	2001:db8:1234:1a00::2b
3	10.0.0.7	198.51.100.3	2001:db8:1234:1a00::3c

Os servidores de banco de dados na sub-rede privada têm os endereços a seguir.

de aplicativos	IPv4 address (Endereço IPv4)	Endereço IPv6
1	10.0.1.5	2001:db8:1234:1a01::1a
2	10.0.1.6	2001:db8:1234:1a01::2b
3	10.0.1.7	2001:db8:1234:1a01::3c

Roteamento

Sua VPC tem um router implícito (mostrado no diagrama de configuração deste cenário). Neste cenário, o assistente de VPC atualiza a tabela de rotas principal usada na sub-rede somente VPN e cria uma tabela de rotas personalizada e a associa à sub-rede pública.

As instâncias em sua sub-rede somente VPN não podem acessar a Internet diretamente; qualquer tráfego vinculado à Internet deve primeiro atravessar o gateway privado virtual até sua rede, onde o tráfego fica sujeito ao seu firewall e às políticas de segurança corporativas. Se as instâncias enviarem qualquer tráfego vinculado à AWS (por exemplo, solicitações ao Amazon S3 ou à APIs do Amazon EC2), as solicitações deverão passar pelo gateway privado virtual até a rede e sair para a Internet, antes de chegar à AWS.

> Tip
>
> E o tráfego que vem de sua rede e vai para uma instância na sub-rede pública por um endereço IP elástico passa pela Internet, e não por um gateway privado virtual. Em vez disso, você poderia configurar uma rota e regras de security group que permitam que o tráfego venha de sua rede por um gateway privado virtual em direção à sub-rede pública.

A conexão Site-to-Site VPN é configurada como uma conexão Site-to-Site VPN com roteamento estático ou como uma conexão Site-to-Site VPN com roteamento dinâmico (que usa BGP). Se você selecionar o roteamento estático, será solicitado a inserir manualmente o prefixo IP da rede ao criar a conexão Site-to-Site VPN. Se você selecionar o roteamento dinâmico, o prefixo IP será anunciado automaticamente para o gateway privado virtual da VPC que usa BGP.

As tabelas a seguir descrevem as tabelas de rotas para este cenário.

Tabela de rotas principal

A primeira entrada é a padrão para roteamento local na VPC; essa entrada permite que as instâncias na VPC comuniquem-se entre si por IPv4. A segunda entrada faz o roteamento de todos os tráfegos IPv4 de sub-rede provenientes da sub-rede privada e direcionados para sua rede por meio do gateway privado virtual (por exemplo, `vgw-1a2b3c4d`).

Destino	Destino
`10.0.0.0/16`	local
`0.0.0.0/0`	vgw-id

Tabela de rotas personalizada

A primeira entrada é a padrão para roteamento local na VPC; essa entrada permite que as instâncias na VPC comuniquem-se entre si. A segunda entrada faz o roteamento de todos os tráfegos IPv4 de sub-rede provenientes da sub-rede pública e direcionados para a Internet por meio do gateway da Internet (por exemplo, `igw-1a2b3c4d`).

Destino	Destino
`10.0.0.0/16`	local
`0.0.0.0/0`	igw-id

Roteamento alternativo

Alternativamente, se desejar que as instâncias na sub-rede privada acessem a Internet, você poderá criar um gateway de conversão de endereços de rede (NAT) ou uma instância na sub-rede pública e configurar o roteamento para que o tráfego vinculado à Internet e direcionado à sub-rede vá para o dispositivo NAT. Isso possibilita que as instâncias na sub-rede somente VPN enviem solicitações pelo gateway da Internet (por exemplo, para atualizações de software).

Para obter mais informações sobre configuração manual de um dispositivo NAT, consulte Dispositivos NAT para sua VPC (p. 228). Para obter mais informações sobre como usar o assistente de VPC para configurar um dispositivo NAT, consulte VPC com sub-redes públicas e privadas (NAT) (p. 31).

Para permitir que o tráfego vinculado à Internet, proveniente da sub-rede privada, vá para o dispositivo NAT, é necessário atualizar a tabela de rotas principal tal como se segue.

A primeira entrada é a padrão para roteamento local na VPC. A segunda entrada roteia o tráfego de sub-rede vinculado à sua própria rede local (cliente) para o gateway privado virtual. Neste exemplo, vamos supor que o intervalo de endereços IP da rede local seja `172.16.0.0/12`. A terceira entrada envia todos os outros tráfegos da sub-rede ao gateway NAT.

Destino	Destino
`10.0.0.0/16`	local
`172.16.0.0/12`	vgw-id
`0.0.0.0/0`	nat-gateway-id

Roteamento para o IPv6

Se você associar um bloco CIDR IPv6 à sua VPC e às sub-redes, a tabela de rotas deverá incluir rotas distintas para tráfego IPv6. As tabelas a seguir mostram a tabela de rotas personalizada para este cenário, se você escolher permitir comunicação IPv6 em sua VPC.

Tabela de rotas principal

A segunda entrada é a rota padrão adicionada automaticamente para roteamento local na VPC via IPv6.

Destino	Destino
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
0.0.0.0/0	vgw-id

Tabela de rotas personalizada

A segunda entrada é a rota padrão adicionada automaticamente para roteamento local na VPC via IPv6. A quarta entrada roteia todos os outros tráfegos IPv6 da sub-rede para o gateway da Internet.

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

A AWS fornece dois recursos que você pode usar para aumentar a segurança da VPC: grupos de segurança e ACLs da rede. Os grupos de segurança controlam o tráfego de entrada e de saída de suas instâncias e as Network ACL controlam o tráfego de entrada e de saída de suas sub-redes. Na maioria dos casos, os grupos de segurança podem atender as suas necessidades; contudo, você também pode usar as Network ACL se desejar uma camada adicional de segurança para o seu VPC. Para obter mais informações, consulte Privacidade do tráfego entre redes na Amazon VPC (p. 158).

No cenário 3, você usará security groups, mas não Network ACLs. Se quiser usar uma network ACL, consulte Regras de network ACL recomendadas para uma VPC com sub-redes públicas e privadas e acesso à AWS Site-to-Site VPN (p. 62).

Sua VPC é fornecida com um security group padrão (p. 181). Uma instância executada na VPC será automaticamente associada ao security group padrão se você não especificar um security group diferente durante a execução. Para este cenário, é recomendável criar os security groups a seguir, em vez de usar o security group padrão:

- WebServerSG: especifique esse security group quando iniciar servidores web na sub-rede pública.
- DBServerSG: especifique esse security group quando iniciar servidores de banco de dados na sub-rede somente VPN.

As instâncias atribuídas a um security group podem estar em diferentes sub-redes. Entretanto, neste cenário, cada security group corresponde ao tipo de função que uma instância desempenha e cada função requer que a instância esteja em uma sub-rede específica. Portanto, neste cenário, todas as instâncias atribuídas a um security group estão na mesma sub-rede.

A tabela a seguir descreve as regras recomendadas para o grupo de segurança WebServerSG, que permitem que os servidores web recebam tráfego da Internet, bem como tráfego SSH e RDP de sua rede. Os servidores web podem também iniciar solicitações de leitura e gravação para os servidores de banco de dados na sub-rede somente VPN e enviar tráfego para a Internet; por exemplo, para obter atualizações de software. Pelo fato de o servidor Web não iniciar nenhuma outra comunicação de saída, a regra de saída padrão é removida.

> **Note**
>
> O grupo inclui acesso SSH e RDP e acesso do Microsoft SQL Server e MySQL. Na sua situação, talvez você precise apenas de regras para o Linux (SSH e MySQL) ou Windows (RDP e Microsoft SQL Server).

WebServerSG: regras recomendadas

Entrada

Origem	Protocolo	Intervalo de portas	Comentários
0.0.0.0/0	TCP	80	Permite acesso HTTP de entrada para servidores web de qualquer endereço IPv4.
0.0.0.0/0	TCP	443	Permite acesso HTTPS de entrada para servidores web de qualquer endereço IPv4.
Intervalo de endereços IP públicos de sua rede	TCP	22	Permite acesso SSH de entrada de sua rede a instâncias Linux (por meio do gateway da Internet).
Intervalo de endereços IP públicos de sua rede	TCP	3389	Permite acesso RDP de entrada de sua rede a instâncias Windows (por meio do gateway da Internet).
Saída			
ID do security group DBServerSG	TCP	1433	Permite acesso de saída do Microsoft SQL Server aos servidores de banco de dados atribuídos ao DBServerSG.
ID do security group DBServerSG	TCP	3306	Permite acesso de saída do MySQL aos servidores de banco de dados atribuídos ao DBServerSG.
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.

A tabela a seguir descreve as regras recomendadas para o security group DBServerSG, que permitem que o Microsoft SQL Server e MySQL leiam e gravem solicitações dos servidores web, bem como tráfego SSH e RDP de sua rede. Os servidores de banco de dados podem também iniciar tráfego vinculado à Internet (sua tabela de rotas envia esse tráfego pelo gateway privado virtual).

DBServerSG: regras recomendadas

Entrada			
Origem	Protocolo	Intervalo de portas	Comentários
ID do security group WebServerSG	TCP	1433	Permite acesso de entrada ao Microsoft SQL Server de servidores web

			associados ao security group WebServerSG.
ID do security group WebServerSG	TCP	3306	Permite acesso de entrada ao MySQL Server de servidores web associados ao security group WebServerSG.
Intervalo de endereços IPv4 de sua rede	TCP	22	Permite tráfego SSH de entrada de sua rede para instâncias Linux (por meio do gateway privado virtual).
Intervalo de endereços IPv4 de sua rede	TCP	3389	Permite tráfego RDP de entrada de sua rede para instâncias Windows (por meio do gateway privado virtual).
Saída			
Destino	Protocolo	Intervalo de portas	Comentários
0.0.0.0/0	TCP	80	Permite acesso HTTP IPv4 de saída à Internet (por exemplo, para atualizações de software) por meio do gateway privado virtual.
0.0.0.0/0	TCP	443	Permite acesso HTTPS IPv4 de saída à Internet (por exemplo, para atualizações de software) por meio do gateway privado virtual.

(Opcional) O security group padrão para uma VPC tem regras que permite automaticamente que as instâncias atribuídas comuniquem-se entre si. Para permitir esse tipo de comunicação a um security group personalizado, é necessário adicionar as regras a seguir:

Entrada			
Origem	Protocolo	Intervalo de portas	Comentários
ID do security group	Tudo	Tudo	(Opcional) Permite tráfego de entrada de outras instâncias atribuídas para esse security group.
Saída			
Destino	Protocolo	Intervalo de portas	Comentários

ID do security group	Tudo	Tudo	Permite tráfego de saída a outras instâncias atribuídas para esse security group.

Regras de grupos de segurança para IPv6

Se você associar um bloco CIDR IPv6 à sua VPC e às sub-redes, deverá adicionar regras distintas aos seus security groups WebServerSG e DBServerSG a fim de controlar o tráfego IPv6 de entrada e saída de suas instâncias. Neste cenário, os servidores web poderão receber todo o tráfego da Internet por IPv6 e tráfego RDP ou SSH de sua rede local por IPv6. Além disso, eles poderão iniciar tráfego IPv6 de saída para a Internet. Os servidores de banco de dados não podem iniciar tráfego IPv6 de saída para a Internet. Por isso, eles não precisam de nenhuma outra regra de grupo de segurança.

A seguir encontram-se regras específicas do IPv6 ao security group WebServerSG (que são um complemento às regras listadas anteriormente).

Entrada			
Origem	Protocolo	Intervalo de portas	Comentários
::/0	TCP	80	Permite acesso HTTP de entrada para servidores web de qualquer endereço IPv6.
::/0	TCP	443	Permite acesso HTTPS de entrada para servidores web de qualquer endereço IPv6.
Intervalo de endereços IPv6 de sua rede	TCP	22	(Instâncias Linux) Permite acesso SSH de entrada de sua rede por IPv6.
Intervalo de endereços IPv6 de sua rede	TCP	3389	(Instâncias Windows) Permite acesso RDP de entrada de sua rede por IPv6
Saída			
Destino	Protocolo	Intervalo de portas	Comentários
::/0	TCP	HTTP	Permite acesso HTTP de saída a qualquer endereço IPv6.
::/0	TCP	HTTPS	Permite acesso HTTPS de saída a qualquer endereço IPv6.

Implementar o cenário 3

Para implementar o cenário 3, obtenha informações sobre seu gateway de cliente e crie a VPC usando o assistente de VPC. O assistente de VPC cria uma conexão Site-to-Site VPN para você com um gateway do cliente e um gateway privado virtual.

Esses procedimentos incluem etapas opcionais para ativar e configurar a comunicação IPv6 para sua VPC. Você não precisa executar essas etapas se não desejar usar IPv6 em sua VPC.

Para preparar o gateway do cliente

1. Determine qual dispositivo você usará como gateway do cliente. Para mais informações, consulte Seu dispositivo de gateway do cliente no Guia do usuário do AWS Site-to-Site VPN.
2. Obtenha o endereço IP roteável na Internet para a interface externa do dispositivo de gateway do cliente. O endereço deve ser estático e pode estar subjacente a um dispositivo que esteja executando conversão de endereços de rede (NAT).
3. Se desejar criar uma conexão Site-to-Site VPN com roteamento estático, obtenha a lista de intervalos de IP (na notação CIDR) que devem ser anunciados na conexão Site-to-Site VPN para o gateway privado virtual. Para mais informações, consulte Tabelas de rotas e prioridade de rotas VPN no Guia do usuário do AWS Site-to-Site VPN.

Para obter informações sobre como usar o assistente da VPC com IPv4, consulte Conceitos básicos (p. 11).

Para obter informações sobre como usar o assistente da VPC com IPv6, consulte the section called “Conceitos básicos do IPv6” (p. 15).

Regras de network ACL recomendadas para uma VPC com sub-redes públicas e privadas e acesso à AWS Site-to-Site VPN

Para esse cenário, você tem uma network ACL para a sub-rede pública e outra network ACL para a sub-rede somente VPN. A tabela a seguir mostra as regras que recomendamos para cada ACL. Elas bloqueiam todos os tráfegos, exceto aquele explicitamente necessário.

Regras de ACL para sub-rede pública

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	PERMISSÃO	Permite tráfego HTTP de entrada para servidores web de qualquer endereço IPv4.
110	0.0.0.0/0	TCP	443	PERMISSÃO	Permite tráfego HTTPS de entrada para servidores web de qualquer endereço IPv4.
120	Intervalo de endereços IPv4	TCP	22	PERMISSÃO	Permite tráfego SSH de entrada para

	públicos de sua rede doméstica				os servidores da web de sua rede doméstica (pelo gateway da Internet).
130	Intervalo de endereços IPv4 públicos de sua rede doméstica	TCP	3389	PERMISSÃO	Permite tráfego RDP de entrada para servidores da web de sua rede doméstica (pelo gateway da Internet).
140	0.0.0.0/0	TCP	32768-65535	PERMISSÃO	Permite tráfego de retorno de entrada de hosts na Internet que estão respondendo a solicitações originadas na sub-rede. O intervalo é apenas de exemplo. Para obter informações sobre como escolher as portas efêmeras corretas para sua configuração, consulte Portas efêmeras (p. 202).
*	0.0.0.0/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos IPv4 de entrada ainda não controlados por uma regra precedente (não modificável).
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments

100	0.0.0.0/0	TCP	80	PERMISSÃO	Permite tráfego HTTP de saída da sub-rede para a Internet.
110	0.0.0.0/0	TCP	443	PERMISSÃO	Permite tráfego HTTPS de saída da sub-rede para a Internet.
120	10.0.1.0/24	TCP	1433	PERMISSÃO	Permite acesso MS SQL de saída a servidores de banco de dados na sub-rede somente VPN. Esse número de porta é apenas de exemplo. Outros exemplos incluem 3306 para acesso MySQL/ Aurora, 5432 para acesso PostgreSQL, 5439 para acesso Amazon Redshift e 1521 para acesso Oracle.

140	0.0.0.0/0	TCP	32768-65535	PERMISSÃO	Permite respostas IPv4 de saída a clientes na Internet (por exemplo, fornece páginas web a pessoas que visitam os servidores web na sub-rede). O intervalo é apenas de exemplo. Para obter informações sobre como escolher as portas efêmeras corretas para sua configuração, consulte Portas efêmeras (p. 202).
*	0.0.0.0/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos de saída ainda não controlados por uma regra precedente (não modificável).

Configurações de ACL para a sub-rede somente VPN

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
100	10.0.0.0/24	TCP	1433	PERMISSÃO	Permite que servidores web na sub-rede pública leiam e gravem em servidores MS SQL na sub-rede somente VPN. Esse número de porta é apenas de

					exemplo. Outros exemplos incluem 3306 para acesso MySQL/ Aurora, 5432 para acesso PostgreSQL, 5439 para acesso Amazon Redshift e 1521 para acesso Oracle.
120	Intervalo de endereços IPv4 privados de sua rede doméstica	TCP	22	PERMISSÃO	Permite tráfego SSH de entrada de sua rede doméstica (no gateway privado virtual).
130	Intervalo de endereços IPv4 privados de sua rede doméstica	TCP	3389	PERMISSÃO	Permite tráfego RDP de entrada de sua rede doméstica (no gateway privado virtual).
140	Intervalo de endereços IP privados de sua rede doméstica	TCP	32768-65535	PERMISSÃO	Permite tráfego de retorno de entrada de clientes na rede doméstica (pelo gateway privado virtual). O intervalo é apenas de exemplo. Para obter informações sobre como escolher as portas efêmeras corretas para sua configuração, consulte Portas efêmeras (p. 202).

*	0.0.0.0/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos de entrada ainda não controlados por uma regra precedente (não modificável).
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
100	Intervalo de endereços IP privados de sua rede doméstica	Tudo	Tudo	PERMISSÃO	Permite todos os tráfegos de saída da sub-rede para sua rede doméstica (no gateway privado virtual). Essa regra também abrange a regra 120. Entretanto, é possível tornar essa regra mais restritiva usando um tipo de protocolo e número de porta específicos. Se você tornar essa regra mais restritiva, deverá incluir a regra 120 em sua network ACL para garantir que as respostas de saída não sejam bloqueadas.

110	10.0.0.0/24	TCP	32768-65535	PERMISSÃO	Permite respostas de saída para servidores web na sub-rede pública. O intervalo é apenas de exemplo. Para obter informações sobre como escolher as portas efêmeras corretas para sua configuração, consulte Portas efêmeras (p. 202).
120	Intervalo de endereços IP privados de sua rede doméstica	TCP	32768-65535	PERMISSÃO	Permite respostas de saída para clientes na rede doméstica (no gateway privado virtual). O intervalo é apenas de exemplo. Para obter informações sobre como escolher as portas efêmeras corretas para sua configuração, consulte Portas efêmeras (p. 202).
*	0.0.0.0/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos de saída ainda não controlados por uma regra precedente (não modificável).

Regras de network ACL recomendadas para IPv6

Se tiver implementado suporte de IPv6 e criado uma VPC e sub-redes com blocos CIDR de IPv6 associados, deverá adicionar regras distintas às suas network ACLs para controlar o tráfego IPv6 de entrada e saída.

Veja a seguir regras específicas de IPv6 para suas network ACLs (que são um complemento às regras precedentes).

Regras de ACL para sub-rede pública

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
150	::/0	TCP	80	PERMISSÃO	Permite tráfego HTTP de entrada de qualquer endereço IPv6.
160	::/0	TCP	443	PERMISSÃO	Permite tráfego HTTPS de entrada de qualquer endereço IPv6.
170	Intervalo de endereços IPv6 de sua rede doméstica	TCP	22	PERMISSÃO	Permite tráfego SSH de entrada por IPv6 de sua rede doméstica (pelo gateway da Internet).
180	Intervalo de endereços IPv6 de sua rede doméstica	TCP	3389	PERMISSÃO	Permite tráfego RDP de entrada por IPv6 de sua rede doméstica (pelo gateway da Internet).
190	::/0	TCP	1024-65535	PERMISSÃO	Permite tráfego de retorno de entrada de hosts na Internet que estão respondendo a solicitações originadas na sub-rede. O intervalo é apenas de exemplo. Para obter informações

					sobre como escolher as portas efêmeras corretas para sua configuração, consulte Portas efêmeras (p. 202).
*	::/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos IPv6 de entrada ainda não controlados por uma regra precedente (não modificável).

Outbound

Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
150	::/0	TCP	80	PERMISSÃO	Permite tráfego HTTP de saída da sub-rede para a Internet.
160	::/0	TCP	443	PERMISSÃO	Permite tráfego HTTPS de saída da sub-rede para a Internet.

170	2001:db8:1234:1a00::/64	TCP	1433	PERMISSÃO	Permite acesso MS SQL de saída a servidores de banco de dados na sub-rede privada. Esse número de porta é apenas de exemplo. Outros exemplos incluem 3306 para acesso MySQL/ Aurora, 5432 para acesso PostgreSQL, 5439 para acesso Amazon Redshift e 1521 para acesso Oracle.
190	::/0	TCP	32768-65535	PERMISSÃO	Permite respostas de saída a clientes na Internet (por exemplo, fornece páginas da web a pessoas que visitam os servidores da web na sub-rede). O intervalo é apenas de exemplo. Para obter informações sobre como escolher as portas efêmeras corretas para sua configuração, consulte Portas efêmeras (p. 202).

*	::/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos IPv6 de saída ainda não controlados por uma regra precedente (não modificável).

Regras de ACL para sub-rede somente VPN

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
150	2001:db8:1234:1a00::/64	TCP	1433	PERMISSÃO	Permite que servidores web na sub-rede pública leiam e gravem em servidores MS SQL na sub-rede privada. Esse número de porta é apenas de exemplo. Outros exemplos incluem 3306 para acesso MySQL/ Aurora, 5432 para acesso PostgreSQL, 5439 para acesso Amazon Redshift e 1521 para acesso Oracle.
*	::/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos IPv6 de entrada ainda não controlados por uma regra precedente (não modificável).
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments

130	2001:db8:1234:1a00::/64	TCP	32768-65535	PERMISSÃO	Permite respostas de saída à sub-rede pública (por exemplo, respostas de servidores web na sub-rede pública que estão se comunicando com servidores de banco de dados na sub-rede privada). O intervalo é apenas de exemplo. Para obter informações sobre como escolher as portas efêmeras corretas para sua configuração, consulte Portas efêmeras (p. 202).
*	::/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos IPv6 de saída ainda não controlados por uma regra precedente (não modificável).

VPC com uma única sub-rede privada e acesso à AWS Site-to-Site VPN

A configuração deste cenário inclui uma virtual private cloud (VPC) com uma única sub-rede privada e um gateway privado virtual para permitir comunicação com sua rede em um túnel VPN IPsec. Não há nenhum Internet Gateway para permitir comunicação na Internet. Recomendamos este cenário se você quiser expandir a rede para a nuvem usando a infraestrutura da Amazon sem expor sua rede à Internet.

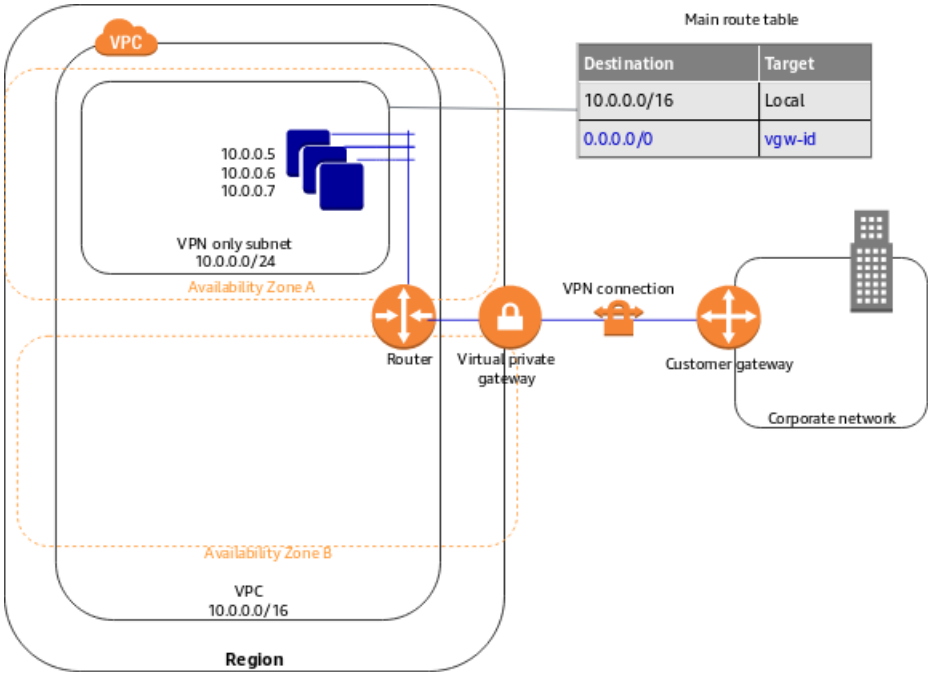
Além disso, este cenário pode ser opcionalmente configurado para IPv6: é possível usar o assistente de VPC para criar uma VPC e uma sub-rede com blocos CIDR IPv6 associados. As instâncias executadas na sub-rede podem receber endereços IPv6. Não oferecemos suporte à comunicação por IPv6 em uma conexão AWS Site-to-Site VPN em um gateway privado virtual. No entanto, as instâncias na VPC podem se comunicar entre si via IPv6. Para obter mais informações sobre endereçamento IPv4 e IPv6, consulte Endereçamento IP na sua VPC (p. 117).

Para obter informações sobre como gerenciar o software de instância do EC2, consulte Gerenciar software na instância do Linux no Guia do usuário do Amazon EC2 para instâncias do Linux.

Tópicos

Visão geral

O diagrama a seguir mostra os principais componentes da configuração deste cenário.



Important

Para esse cenário, consulte Seu dispositivo de gateway do cliente para configurar o dispositivo de gateway do cliente no seu lado da conexão Site-to-Site VPN.

A configuração deste cenário inclui o seguinte:

- Uma virtual private cloud (VPC) com CIDR tamanho /16 (exemplo: 10.0.0.0/16). Nesse caso, são fornecidos 65.536 endereços IP privados.
- Sub-rede somente VPN com CIDR tamanho /24 (exemplo: 10.0.0.0/24). Nesse caso, são fornecidos 256 endereços IP privados.
- Conexão Site-to-Site VPN entre a VPC e a rede. A conexão Site-to-Site VPN compreende um gateway privado virtual localizado na conexão Site-to-Site VPN do lado da Amazon e um gateway do cliente localizado na conexão Site-to-Site VPN do seu lado.
- As instâncias com endereços IP privados no intervalo da sub-rede (exemplos: 10.0.0.5, 10.0.0.6 e 10.0.0.7). Isso permite que as instâncias se comuniquem entre si e com outras instâncias na VPC.
- A tabela de rotas principal contém uma rota que permite que as instâncias na sub-rede se comuniquem com outras instâncias na VPC. A propagação da rota está habilitada, portanto, uma rota que permite que as instâncias na sub-rede se comuniquem diretamente com sua rede aparece como uma rota propagada na tabela de rotas principal.

Para obter mais informações sobre sub-redes, consulte VPCs e sub-redes (p. 100) e Endereçamento IP na sua VPC (p. 117). Para mais informações sobre a conexão do Site-to-Site VPN, consulte O que é o AWS Site-to-Site VPN? no Guia do usuário do AWS Site-to-Site VPN. Para obter mais informações sobre como configurar um dispositivo de gateway do cliente, consulte Seu dispositivo de gateway do cliente.

Visão geral de IPv6

Opcionalmente, você pode ativar o IPv6 para este cenário. Além dos componentes listados anteriormente, a configuração inclui o seguinte:

- Um bloco CIDR IPv6 tamanho /56 associado à VPC (exemplo: 2001:db8:1234:1a00::/56). A AWS atribui automaticamente o CIDR; não é possível escolher o intervalo.
- Um bloco CIDR IPv6 tamanho /64 associado a uma sub-rede somente VPN (exemplo: 2001:db8:1234:1a00::/64). Você pode escolher o intervalo para sua sub-rede com base no intervalo alocado à VPC. Você não pode escolher o tamanho do CIDR IPv6.
- Endereços IPv6 atribuídos às instâncias no intervalo da sub-rede (exemplo: 2001:db8:1234:1a00::1a).
- Uma entrada da tabela de rotas principal que permite que as instâncias na sub-rede privada usem IPv6 para se comunicarem entre si.

Roteamento

Sua VPC tem um router implícito (mostrado no diagrama de configuração deste cenário). Neste cenário, o assistente de VPC cria uma tabela de rotas que roteia todos os tráfegos destinados para um endereço fora da VPC para a conexão AWS Site-to-Site VPN e associa a tabela de rotas à sub-rede.

A seguir é apresentada a tabela de rotas para esse cenário. A primeira entrada é a padrão para um roteamento local na VPC; essa entrada permite que as instâncias na VPC comuniquem-se entre si. A segunda entrada roteia todos os outros tráfegos da sub-rede ao gateway privado virtual (por exemplo, `vgw-1a2b3c4d`).

Destino	Destino
10.0.0.0/16	local
0.0.0.0/0	vgw-id

A conexão AWS Site-to-Site VPN é configurada como uma conexão Site-to-Site VPN com roteamento estático ou como uma conexão Site-to-Site VPN com roteamento dinâmico (que usa BGP). Se você selecionar o roteamento estático, será solicitado a inserir manualmente o prefixo IP da rede ao criar a conexão Site-to-Site VPN. Se você selecionar roteamento dinâmico, o prefixo IP será anunciado automaticamente para sua VPC por meio do BGP.

As instâncias em sua VPC não podem acessar a Internet diretamente; qualquer tráfego vinculado à Internet deve primeiro atravessar o gateway privado virtual até sua rede, onde o tráfego fica sujeito ao seu firewall e às políticas de segurança corporativas. Se as instâncias enviarem qualquer tráfego vinculado à AWS (por exemplo, solicitações para o Amazon S3 ou o Amazon EC2), as solicitações deverão passar pelo gateway privado virtual até a rede e depois para a Internet, antes de chegar à AWS.

Roteamento para o IPv6

Se você associar um bloco CIDR IPv6 à sua VPC e às sub-redes, a tabela de rotas incluirá rotas distintas para o tráfego IPv6. A seguir é apresentada a tabela de rotas personalizada para esse cenário. A segunda entrada é a rota padrão adicionada automaticamente para roteamento local na VPC via IPv6.

Destino	Destino
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
0.0.0.0/0	vgw-id

Segurança

A AWS fornece dois recursos que você pode usar para aumentar a segurança da VPC: grupos de segurança e ACLs da rede. Os grupos de segurança controlam o tráfego de entrada e de saída de suas instâncias e as Network ACL controlam o tráfego de entrada e de saída de suas sub-redes. Na maioria dos casos, os grupos de segurança podem atender as suas necessidades; contudo, você também pode usar as Network ACL se desejar uma camada adicional de segurança para o seu VPC. Para obter mais informações, consulte Privacidade do tráfego entre redes na Amazon VPC (p. 158).

No cenário 4, você usará o security group padrão para sua VPC, mas não para uma Network ACL. Se quiser usar uma network ACL, consulte Regras de network ACL recomendadas para uma VPC com apenas uma sub-rede privada e acesso à AWS Site-to-Site VPN (p. 77).

Sua VPC vem com um security group padrão cujas configurações iniciais negam todos os tráfegos de entrada, permitem todos os tráfegos de saída e permitem todos os tráfegos entre as instâncias atribuídas ao security group. Para esse cenário, é recomendável adicionar regras de entrada ao security group padrão para permitir trafego SSH (Linux) e tráfego Remote Desktop (Windows) de sua rede.

> **Important**
>
> O security group padrão automaticamente permite que as instâncias atribuídas comuniquem-se entre si. Portanto, você não precisa adicionar uma regra para isso. Se você usar um security group diferente, deverá adicionar uma regra que dê essa permissão.

A tabela a seguir descreve as regras de entrada que você deve adicionar ao security group padrão de sua VPC.

Grupo de segurança padrão: regras recomendadas

Entrada			
Origem	Protocolo	Intervalo de portas	Comentários
Intervalo de endereços IPv4 privados de sua rede	TCP	22	(Instâncias Linux) Permite tráfego SSH de entrada de sua rede.
Intervalo de endereços IPv4 privados de sua rede	TCP	3389	(Instâncias Windows) Permite tráfego RDP de entrada de sua rede.

Regras de grupos de segurança para IPv6

Se você associar um bloco CIDR IPv6 à sua VPC e às sub-redes, deverá adicionar regras distintas ao seu security group a fim de controlar o tráfego IPv6 de entrada e saída de suas instâncias. Nesse cenário, os servidores de banco de dados não podem ser acessados por meio da conexão Site-to-Site VPN usando IPv6; por isso, não há necessidade de nenhuma regra adicional de grupo de segurança.

Regras de network ACL recomendadas para uma VPC com apenas uma sub-rede privada e acesso à AWS Site-to-Site VPN

A tabela a seguir mostra as regras que recomendamos. Elas bloqueiam todos os tráfegos, exceto aquele explicitamente necessário.

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
100	Intervalo de endereços IP privados de sua rede doméstica	TCP	22	PERMISSÃO	Permite tráfego SSH de entrada de sua rede doméstica para a sub-rede.
110	Intervalo de endereços IP privados de sua rede doméstica	TCP	3389	PERMISSÃO	Permite tráfego RDP de entrada de sua rede doméstica para a sub-rede.
120	Intervalo de endereços IP privados de sua rede doméstica	TCP	32768-65535	PERMISSÃO	Permite tráfego de retorno de entrada de solicitações originadas na sub-rede. O intervalo é apenas de exemplo. Para obter informações sobre como escolher as portas efêmeras corretas para sua configuração, consulte Portas efêmeras (p. 202).
*	0.0.0.0/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos de entrada ainda não controlados por uma regra precedente (não modificável).
Outbound					

Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
100	Intervalo de endereços IP privados de sua rede doméstica	Tudo	Tudo	PERMISSÃO	Permite todos os tráfegos de saída da sub-rede para sua rede doméstica. Essa regra também abrange a regra 120. Entretanto, é possível tornar essa regra mais restritiva usando um tipo de protocolo e número de porta específicos. Se você tornar essa regra mais restritiva, deverá incluir a regra 120 em sua network ACL para garantir que as respostas de saída não sejam bloqueadas.
120	Intervalo de endereços IP privados de sua rede doméstica	TCP	32768-65535	PERMISSÃO	Permite respostas de saída para clientes na rede doméstica. O intervalo é apenas de exemplo. Para obter informações sobre como escolher as portas efêmeras corretas para sua configuração, consulte Portas efêmeras (p. 202).

*	0.0.0.0/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos de saída ainda não controlados por uma regra precedente (não modificável).

Regras de network ACL recomendadas para IPv6

Se tiver implementado o cenário 4 com o suporte de IPv6 e criado uma VPC e uma sub-rede com blocos CIDR de IPv6 associados, deverá adicionar regras distintas à Network ACL para controlar o tráfego IPv6 de entrada e saída.

Nesse cenário, os servidores de banco de dados não podem ser acessados por comunicação VPN via IPv6. Por isso, não há necessidade de nenhuma regra adicional de Network ACL. A seguir encontram-se regras padrão que negam tráfego IPv6 para e proveniente da sub-rede.

Regras de ACL para sub-rede somente VPN

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
*	::/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos IPv6 de entrada ainda não controlados por uma regra precedente (não modificável).
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
*	::/0	tudo	tudo	NEGAÇÃO	Nega todos os tráfegos IPv6 de saída ainda não controlados por uma regra precedente (não modificável).

Exemplos para a VPC

Esta seção tem exemplos de como criar e configurar uma VPC.

Exemplo	Uso
Exemplo: criação de uma VPC para IPv4 e de sub-redes usando a CLI da AWS (p. 85)	Use a CLI da AWS para criar uma VPC com uma sub-rede pública e uma sub-rede privada.
Exemplo: criação de uma VPC para IPv6 e de sub-redes usando a CLI da AWS (p. 91)	Use a CLI da AWS para criar uma VPC com um bloco CIDR IPv6 associado, uma sub-rede pública e uma sub-rede privada, cada uma com um bloco CIDR IPv6 associado.
the section called “Exemplo: Compartilhar sub-redes públicas e privadas” (p. 81)	Compartilhe sub-redes públicas e privadas com as contas.
the section called “Exemplo: serviços usando o AWS PrivateLink e o emparelhamento de VPC” (p. 81)	Saiba como usar uma combinação de emparelhamento de VPC e o AWS PrivateLink para estender o acesso a serviços privados para os consumidores.

Também é possível usar um gateway de trânsito para conectar as VPCs.

Exemplo	Uso
Roteador centralizado	É possível configurar o gateway de trânsito como um roteador centralizado que conecta todas as conexões de VPCs, do AWS Direct Connect e AWS Site-to-Site VPN. Para obter mais informações sobre como configurar o gateway de trânsito como um roteador centralizado, consulte Exemplo de gateway de trânsito: roteador centralizado em Gateways de trânsito da Amazon VPC.
VPCs isoladas	É possível configurar o gateway de trânsito 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. Para obter mais informações sobre como configurar o gateway de trânsito para isolar as VPCs, consulte Exemplo de gateway de trânsito: VPCs isoladas em Gateways de trânsito da Amazon VPC.
VPCs isoladas com serviços compartilhados	É possível configurar o gateway de trânsito como vários roteadores isolados que usam um serviço compartilhado. É parecido com usar vários gateways de trânsito, mas permite mais flexibilidade nos casos em que roteadores e anexos podem mudar. Para obter mais informações sobre como configurar o gateway de trânsito para isolar as VPCs, consulte Exemplo de gateway

Exemplo	Uso
	de trânsito: VPCs isoladas com os serviços compartilhados em Gateways de trânsito da Amazon VPC.

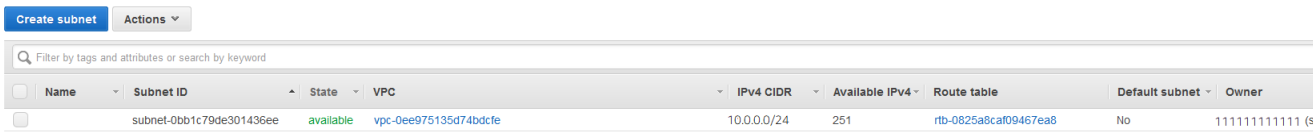
Exemplo: Compartilhar sub-redes públicas e privadas

Considere um cenário em que você deseje que uma conta seja responsável pela infraestrutura, incluindo sub-redes, tabelas de rotas, gateway e intervalos de CIDR, e que outras contas na mesma AWS Organization usem as sub-redes. O proprietário da VPC (conta A) cria uma infraestrutura de roteamento, incluindo VPCs, sub-redes, tabelas de rotas, gateways e ACLs de rede. A conta D quer criar aplicativos de interação com o público. As contas B e C querem criar aplicativos privados que não precisam estar conectados à Internet e que residam em sub-redes privadas. A conta A pode usar o AWS Resource Access Manager para criar um compartilhamento de recursos para as sub-redes e, depois, compartilhar as sub-redes. A conta A compartilha as sub-redes públicas e privadas com a conta D e as sub-redes privadas com as conta B e C. As contas B, C e D podem criar recursos nas sub-redes. Cada conta pode ver somente as sub-redes compartilhadas com ela; por exemplo, a conta D só pode ver sub-redes privadas. Cada uma das contas pode controlar seus próprios recursos, incluindo instâncias e grupos de segurança.

A conta A gerencia a infraestrutura de IP, incluindo as tabelas de rotas para as sub-redes públicas e privadas. Não é necessária nenhuma configuração adicional para sub-redes compartilhadas. Portanto, as tabelas de rotas são as mesmas das sub-redes não compartilhadas.

A conta A (ID da conta 111111111111) compartilha a sub-rede pública com a conta D (444444444444). A conta D vê a seguinte sub-rede e a coluna Proprietário exibe dois indicadores de que a sub-rede é compartilhada.

- O ID da conta A é o proprietário da VPC (111111111111) e é diferente do ID da conta D (444444444444).
- A palavra "shared" (Compartilhada) aparece ao lado do ID da conta proprietária.



Exemplo: serviços usando o AWS PrivateLink e o emparelhamento de VPC

O provedor de serviços do AWS PrivateLink configura instâncias para executar serviços na VPC, usando um Network Load Balancer como front-end. Use o emparelhamento de VPC entre regiões (VPCs que estão na mesma região) e o emparelhamento de VPC entre regiões (VPCs que estão em regiões diferentes) com o AWS PrivateLink para conceder acesso privado aos consumidores em todas as conexões de emparelhamento de VPC.

Os consumidores em VPCs remotas não podem usar os nomes DNS privados nas conexões emparelhadas. No entanto, podem criar a própria zona hospedada privada em Route 53 e anexá-la às

VPCs para usar o mesmo nome do DNS privado. Para obter informações sobre como usar o gateway de trânsito com o Amazon Route 53 Resolver para compartilhar endpoints de interface do PrivateLink entre várias VPCs conectadas e um ambiente on-premise, consulte Integrar o AWS Transit Gateway ao AWS PrivateLink e ao Amazon Route 53 Resolver.

Veja a seguir exemplos de configuração usando o AWS PrivateLink e o emparelhamento de VPC.

Exemplos

Recursos adicionais

Os tópicos a seguir podem ajudar você a configurar os componentes necessários para os exemplos:

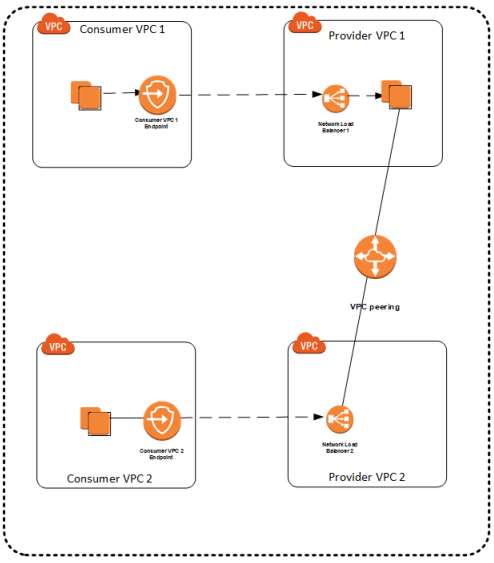
- Serviços do VPC endpoint
- Conceitos básicos sobre Network Load Balancers.
- Trabalhar com conexões de emparelhamento de VPC
- Para criar um endpoint de interface

Para obter mais exemplos de emparelhamento de VPC, consulte os tópicos a seguir no Guia de emparelhamento da Amazon VPC:

- Configurações de emparelhamento de VPC
- Configurações de emparelhamento de VPC sem suporte

Exemplo: O provedor do serviço configura o serviço

No exemplo a seguir, um serviço é executado em instâncias da VPC 1 do provedor. Os recursos que estão na VPC 1 do consumidor podem acessar o serviço por meio de um endpoint de interface na VPC1 do consumidor.

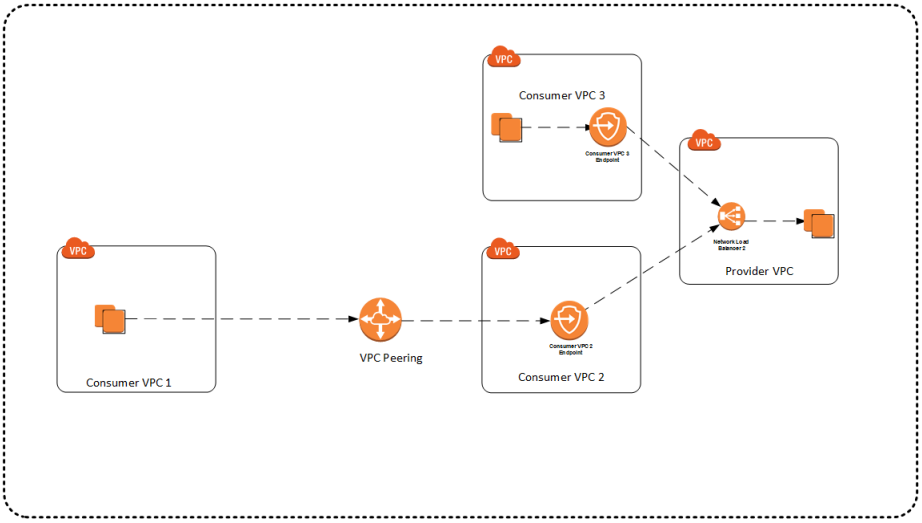


Para permitir que os recursos que estão na VPC 2 do consumidor acessem o serviço de maneira privada, o provedor do serviço deve concluir as seguintes etapas:

1. Crie a VPC 2 do provedor.
2. Crie a conexão de emparelhamento de VPC entre as VPCs 1 e 2 do provedor, para que o tráfego possa ser roteado entre as duas VPCs. Para obter mais informações, consulte Criar e aceitar uma conexão de emparelhamento de VPC.
3. Criar um Network Load Balancer 2 na VPC do provedor 2. Para obter mais informações, consulte Conceitos básicos dos Network Load Balancers.
4. Criar um grupo de destino. Para obter mais informações, consulte Criar um grupo de destino para o Network Load Balancer.
5. Configurar grupos de destino no Network Load Balancer 2 que apontem para os endereços IP das instâncias de serviço na VPC de provedor 1. Para obter mais informações, consulte Registrar destinos com seu grupo de destino.
6. Ajustar os grupos de segurança associados às instâncias de serviço na VPC de provedor 1, para que elas permitam o tráfego do Network Load Balancer 2. Para obter mais informações, consulte Grupos de segurança de destino.
7. Criar uma configuração de serviço VPC endpoint na VPC de provedor 2 e associá-la ao Network Load Balancer 2. Para obter mais informações, consulte Criar uma configuração de serviço de VPC endpoint.
8. O consumidor de serviço poderá criar um endpoint de interface na VPC de consumidor 2 para o serviço na VPC de provedor 2. Para obter mais informações, consulte Criar um endpoint de interface.

Exemplo: O consumidor do serviço configura o acesso

No exemplo a seguir, um serviço é executado em instâncias da VPC do provedor. Os recursos que estão na VPC 3 do consumidor podem acessar o serviço diretamente por meio de um endpoint de interface na VPC 3 do consumidor.



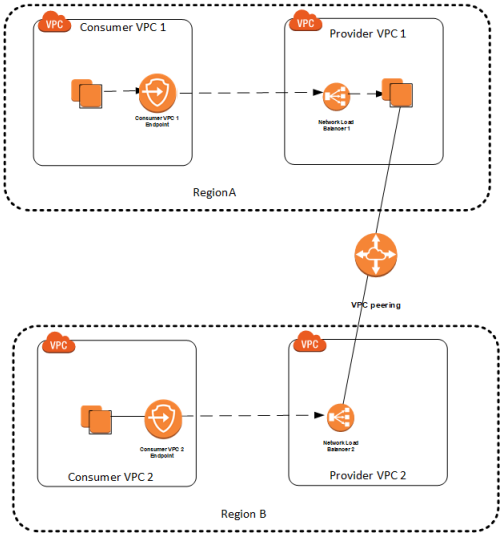
Para permitir que os recursos na VPC de consumidor 1 acessem o serviço de forma privada (sem criar um endpoint de interface diretamente na VPC de consumidor 1), o consumidor de serviço pode fazer o seguinte:

1. Crie a VPC 2 do consumidor.
2. Crie um endpoint de interface que abranja uma ou mais sub-redes na VPC 2 do consumidor. Para obter mais informações, consulte Criar um endpoint de interface.

3. Verifique se os grupos de segurança associados ao endpoint de interface na VPC 2 do consumidor permitem o tráfego das instâncias na VPC 1 do consumidor. Verifique se os grupos de segurança associados às instâncias na VPC 1 do consumidor permitem o tráfego para o endpoint da interface na VPC 2 do consumidor.
4. Crie a conexão de emparelhamento de VPC entre as VPCs 1 e 2 do consumidor, para que o tráfego seja roteado entre as duas VPCs. Para obter mais informações, consulte Criar e aceitar uma conexão de emparelhamento de VPC.

Exemplo: O provedor do serviço configura um serviço para operar em várias regiões

No seguinte exemplo, um serviço é executado em instâncias da VPC 1 do provedor na região A (por exemplo, us-east-1). Os recursos da VPC 1 do consumidor presentes na mesma região podem acessar o serviço diretamente por um endpoint de interface na VPC 1 do consumidor.



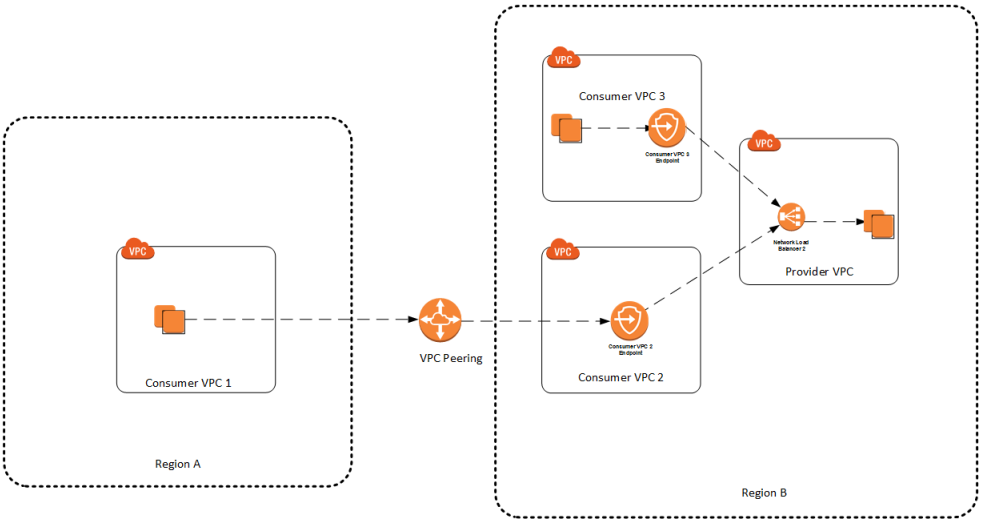
Para permitir que os recursos da VPC 2 do consumidor na região B (por exemplo, eu-west-1) acessem o serviço de maneira privada, o provedor do serviço deve realizar as seguintes etapas:

1. Criar uma VPC de provedor 2 na região B.
2. Crie a conexão de emparelhamento de VPC entre regiões entre as VPCs 1 e 2 do provedor, para que o tráfego possa ser roteado entre as duas VPCs. Para obter mais informações, consulte Criar e aceitar uma conexão de emparelhamento de VPC.
3. Criar um Network Load Balancer 2 na VPC do provedor 2. Para obter mais informações, consulte Conceitos básicos dos Network Load Balancers.
4. Configurar grupos de destino no Network Load Balancer 2 que apontem para os endereços IP das instâncias de serviço na VPC de provedor 1. Para obter mais informações, consulte Registrar destinos com seu grupo de destino.
5. Ajustar os grupos de segurança associados às instâncias de serviço na VPC de provedor 1, para que elas permitam o tráfego do Network Load Balancer 2. Para obter mais informações, consulte Grupos de segurança de destino.
6. Criar uma configuração de serviço VPC endpoint na VPC de provedor 2 e associá-la ao Network Load Balancer 2. Para obter mais informações, consulte Criar uma configuração de serviço de VPC endpoint.
7. O consumidor de serviço poderá criar um endpoint de interface na VPC de consumidor 2 para o serviço na VPC de provedor 2. Para obter mais informações, consulte Criar um endpoint de interface.

A conta com a VPC 2 do provedor incorre nas cobranças de transferência de dados de emparelhamento entre regiões e cobranças do Network Load Balancer. A conta com a VPC 1 do provedor incorre nas cobranças das instâncias de serviço.

Exemplo: O consumidor do serviço configura o acesso em várias regiões

No seguinte exemplo, um serviço é executado em instâncias na VPC do provedor na região B, por exemplo, us-east-1. Os recursos que estão na VPC 3 do consumidor podem acessar o serviço diretamente por meio de um endpoint de interface na VPC 3 do consumidor.



Para permitir que os recursos que estão na VPC 1 do consumidor acessem o serviço de maneira privada, o consumidor do serviço deve concluir as seguintes etapas:

1. Criar uma VPC 2 de consumidor na região B.
2. Crie um endpoint de interface que abranja uma ou mais sub-redes na VPC 2 do consumidor. Para obter mais informações, consulte Criar um endpoint de interface.
3. Certifique-se de que os grupos de segurança associados ao endpoint de interface na VPC 2 do consumidor permitam o tráfego das instâncias na VPC 1 do consumidor. Certifique-se de que os grupos de segurança associados às instâncias na VPC 1 do consumidor permitam o tráfego para o endpoint de interface na VPC 2 do consumidor.
4. Crie o emparelhamento de VPC entre regiões entre as VPCs 1 e 2 do consumidor, para que o tráfego seja roteado entre as duas VPCs. Para obter mais informações, consulte Criar e aceitar uma conexão de emparelhamento de VPC.

A conta do consumidor será cobrada pela transferência de dados no emparelhamento entre regiões e pelas horas e pelo processamento de dados no VPC endpoint. O provedor será cobrado pelo Network Load Balancer e pelas instâncias de serviço.

Exemplo: criação de uma VPC para IPv4 e de sub-redes usando a CLI da AWS

O exemplo a seguir usa comandos da CLI da AWS para criar uma VPC não padrão com um bloco CIDR IPv4, uma sub-rede pública e uma sub-rede privada na VPC. Depois que criar a VPC e as sub-redes, você

pode executar uma instância na sub-rede pública e conectar-se a ela. Para começar, é necessário primeiro instalar e configurar a CLI da AWS. Para obter mais informações, consulte: Instalar a CLI da AWS.

Você criará os seguintes recursos da AWS:

- Uma VPC
- Duas sub-redes
- Um gateway de Internet
- Uma tabela de rotas
- Uma instância do EC2

Tarefas

Etapa 1: Criar uma VPC e sub-redes

A primeira etapa é criar uma VPC e duas sub-redes. Esse exemplo usa o bloco CIDR `10.0.0.0/16` para a VPC, mas você pode escolher um bloco CIDR diferente. Para obter mais informações, consulte Dimensionamento da VPC e da sub-rede (p. 103).

Como criar uma VPC e sub-redes usando a CLI da AWS

1. Crie uma VPC com um bloco CIDR `10.0.0.0/16`.

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16
```

   Na saída retornada, anote o ID da VPC.

```
{
    "Vpc": {
        "VpcId": "vpc-2f09a348",
        ...
    }
}
```

2. Usando o ID da VPC da etapa anterior, crie uma sub-rede com um bloco CIDR `10.0.1.0/24`.

```
aws ec2 create-subnet --vpc-id vpc-2f09a348 --cidr-block 10.0.1.0/24
```

3. Crie uma segunda sub-rede na VPC com um bloco CIDR `10.0.0.0/24`.

```
aws ec2 create-subnet --vpc-id vpc-2f09a348 --cidr-block 10.0.0.0/24
```

Etapa 2: Tornar a sub-rede pública

Assim que criar a VPC e as sub-redes, poderá tornar uma das sub-redes uma sub-rede pública, anexando um gateway da Internet à sua VPC, criando uma tabela de rotas personalizada e configurando o roteamento da sub-rede para o Gateway da internet.

Para tornar sua sub-rede uma sub-rede pública

1. Crie um gateway da Internet.

```
aws ec2 create-internet-gateway
```

   Na saída retornada, anote o ID do Internet Gateway.

```
{
    "InternetGateway": {
        ...
        "InternetGatewayId": "igw-1ff7a07b",
        ...
    }
}
```

2. Usando o ID da etapa anterior, anexe o Internet Gateway à sua VPC.

```
aws ec2 attach-internet-gateway --vpc-id vpc-2f09a348 --internet-gateway-
id igw-1ff7a07b
```

3. Crie uma tabela de rotas personalizada para sua VPC.

```
aws ec2 create-route-table --vpc-id vpc-2f09a348
```

   Na saída retornada, anote o ID da tabela de rotas.

```
{
    "RouteTable": {
        ...
        "RouteTableId": "rtb-c1c8faa6",
        ...
    }
}
```

4. Crie uma rota na tabela de rotas que direcione todo o tráfego (`0.0.0.0/0`) para o Gateway da Internet.

```
aws ec2 create-route --route-table-id rtb-c1c8faa6 --destination-cidr-block 0.0.0.0/0
 --gateway-id igw-1ff7a07b
```

5. Para confirmar se a rota foi criada e está ativa, você pode descrever a tabela de rotas e visualizar os resultados.

```
aws ec2 describe-route-tables --route-table-id rtb-c1c8faa6
```

```
{
    "RouteTables": [
        {
            "Associations": [],
            "RouteTableId": "rtb-c1c8faa6",
            "VpcId": "vpc-2f09a348",
            "PropagatingVgws": [],
            "Tags": [],
            "Routes": [
                {
                    "GatewayId": "local",
                    "DestinationCidrBlock": "10.0.0.0/16",
```

```
                    "State": "active",
                    "Origin": "CreateRouteTable"
                },
                {
                    "GatewayId": "igw-1ff7a07b",
                    "DestinationCidrBlock": "0.0.0.0/0",
                    "State": "active",
                    "Origin": "CreateRoute"
                }
            ]
        }
    ]
}
```

6. No momento, a tabela de rotas não está associada a nenhuma sub-rede. É preciso associá-la a uma sub-rede em sua VPC para que o tráfego dessa sub-rede seja roteado para o Gateway da Internet. Primeiro, use o comando `describe-subnets` para obter seus IDs de sub-rede. Você pode usar a opção `--filter` para retornar as sub-redes apenas para sua nova VPC e a opção `--query` para retornar somente os IDs de sub-rede e seus respectivos blocos CIDR.

```
aws ec2 describe-subnets --filters "Name=vpc-id,Values=vpc-2f09a348" --query
 'Subnets[*].{ID:SubnetId,CIDR:CidrBlock}'
```

```
[
    {
        "CIDR": "10.0.1.0/24",
        "ID": "subnet-b46032ec"
    },
    {
        "CIDR": "10.0.0.0/24",
        "ID": "subnet-a46032fc"
    }
]
```

7. Você pode escolher com qual sub-rede deseja associar a tabela de rotas personalizada; por exemplo, `subnet-b46032ec`. Essa sub-rede será sua sub-rede pública.

```
aws ec2 associate-route-table  --subnet-id subnet-b46032ec --route-table-id rtb-
c1c8faa6
```

8. Você pode, opcionalmente, modificar o comportamento do endereçamento IP público da sua sub-rede para que uma instância executada na sub-rede receba, automaticamente, um endereço IP público. Caso contrário, associe um endereço IP elástico à sua instância depois que for executada, para que fique acessível na Internet.

```
aws ec2 modify-subnet-attribute --subnet-id subnet-b46032ec --map-public-ip-on-launch
```

Etapa 3: Executar uma instância na sub-rede

Para testar se sua sub-rede é pública e se as instâncias na sub-rede são acessíveis pela Internet, execute uma instância em sua sub-rede pública e conecte-se a ela. Primeiro, você precisa criar um security group para ser associado com sua instância e um par de chaves com o qual você se conectará à sua instância. Para mais informações sobre security groups, consulte Grupos de segurança para a VPC (p. 180). Para obter mais informações sobre pares de chaves, consulte Pares de chaves do Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias do Linux.

Para executar e conectar-se a uma instância em sua sub-rede pública

1. Crie um par de chaves e use a opção `--query` e a opção de texto `--output` para canalizar sua chave privada diretamente em um arquivo com a extensão `.pem`.

```
aws ec2 create-key-pair --key-name MyKeyPair --query 'KeyMaterial' --output text
 > MyKeyPair.pem
```

   Neste exemplo, execute uma instância do Amazon Linux. Se você usar um cliente SSH em um sistema operacional Linux ou Mac OS X para se conectar à sua instância, use o seguinte comando para definir as permissões do arquivo de chave privada, de maneira que apenas você possa lê-lo.

```
chmod 400 MyKeyPair.pem
```

2. Crie um security group na sua VPC e adicione uma regra que permita o acesso SSH de qualquer lugar.

```
aws ec2 create-security-group --group-name SSHAccess --description "Security group for
 SSH access" --vpc-id vpc-2f09a348
```

```
{
    "GroupId": "sg-e1fb8c9a"
}
```

```
aws ec2 authorize-security-group-ingress --group-id sg-e1fb8c9a --protocol tcp --
port 22 --cidr 0.0.0.0/0
```

   Note

   Se usar `0.0.0.0/0`, permitirá que todos os endereços IPv4 acessem sua instância usando SSH. Isso é aceitável para esse breve exercício. Porém, na produção, autorize somente um endereço IP específico ou um intervalo de endereços.

3. Execute uma instância em sua sub-rede pública, usando o security group e o par de chaves que você criou. Examine o resultado e anote o ID de sua instância.

```
aws ec2 run-instances --image-id ami-a4827dc9 --count 1 --instance-type t2.micro --key-
name MyKeyPair --security-group-ids sg-e1fb8c9a --subnet-id subnet-b46032ec
```

   Note

   Neste exemplo, a AMI é uma AMI do Amazon Linux na região Leste dos EUA (Norte da Virgínia). Se estiver em uma região diferente, precisará do ID de uma AMI adequado à sua região. Para obter mais informações, consulte Encontrar uma AMI do Linux no Guia do usuário do Amazon EC2 para instâncias do Linux.

4. Sua instância precisa estar no estado `running` para você se conectar a ela. Descreva sua instância, confirme o estado dela e tome nota do respectivo endereço IP público.

```
aws ec2 describe-instances --instance-id i-0146854b7443af453
```

```
{
    "Reservations": [
        {
            ...
            "Instances": [
```

```
                {
                    ...
                    "State": {
                        "Code": 16,
                        "Name": "running"
                    },
                    ...
                    "PublicIpAddress": "52.87.168.235",
                    ...
                }
            ]
        }
    ]
}
```

5. Quando sua instância estiver no estado de execução, você poderá conectar-se a ela usando um cliente SSH em um computador Linux ou Mac OS X por meio do seguinte comando:

```
ssh -i "MyKeyPair.pem" ec2-user@52.87.168.235
```

   Se você estiver se conectando de um computador Windows, use as instruções a seguir: Conectar-se à instância do Linux no Windows utilizando PuTTY.

Etapa 4: Limpeza

Depois de verificar se está conectado à sua instância, você poderá encerrá-la se não for mais necessária. Para isso, use o comando terminate-instances. Par excluir os outros recursos que você criou neste exemplo, use os comandos a seguir na ordem em que são listados:

1. Exclua seu security group:

```
aws ec2 delete-security-group --group-id sg-e1fb8c9a
```

2. Exclua suas sub-redes:

```
aws ec2 delete-subnet --subnet-id subnet-b46032ec
```

```
aws ec2 delete-subnet --subnet-id subnet-a46032fc
```

3. Exclua sua tabela de rotas personalizada:

```
aws ec2 delete-route-table --route-table-id rtb-c1c8faa6
```

4. Exclua o Internet Gateway da VPC:

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-1ff7a07b --vpc-id vpc-2f09a348
```

5. Exclua seu Internet Gateway:

```
aws ec2 delete-internet-gateway --internet-gateway-id igw-1ff7a07b
```

6. Exclua sua VPC:

```
aws ec2 delete-vpc --vpc-id vpc-2f09a348
```

Exemplo: criação de uma VPC para IPv6 e de sub-redes usando a CLI da AWS

O exemplo a seguir usa comandos da CLI da AWS para criar uma VPC não padrão com um bloco CIDR IPv6, uma sub-rede pública e uma sub-rede privada com apenas acesso de saída à Internet. Depois que criar a VPC e as sub-redes, você pode executar uma instância na sub-rede pública e conectar-se a ela. Você pode executar uma instância em sua sub-rede privada e verificar se ela consegue se conectar à Internet. Para começar, é necessário primeiro instalar e configurar a CLI da AWS. Para obter mais informações, consulte: Instalar a CLI da AWS.

Você criará os seguintes recursos da AWS:

- Uma VPC
- Duas sub-redes
- Um gateway de Internet
- Uma tabela de rotas
- Uma instância do EC2

Tarefas

Etapa 1: Criar uma VPC e sub-redes

A primeira etapa é criar uma VPC e duas sub-redes. Esse exemplo usa o bloco CIDR IPv4 `10.0.0.0/16` para a VPC, mas você pode escolher um bloco CIDR diferente. Para obter mais informações, consulte Dimensionamento da VPC e da sub-rede (p. 103).

Como criar uma VPC e sub-redes usando a CLI da AWS

1. Crie uma VPC com um bloco CIDR `10.0.0.0/16` e associe um bloco CIDR IPv6 à VPC.

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --amazon-provided-ipv6-cidr-block
```

   Na saída retornada, anote o ID da VPC.

```
{
    "Vpc": {
        "VpcId": "vpc-2f09a348",
        ...
}
```

2. Descreve sua VPC para obter o bloco CIDR IPv6 associado à VPC.

```
aws ec2 describe-vpcs --vpc-id vpc-2f09a348
```

```
{
    "Vpcs": [
        {
            ...
            "Ipv6CidrBlockAssociationSet": [
                {
                    "Ipv6CidrBlock": "2001:db8:1234:1a00::/56",
                    "AssociationId": "vpc-cidr-assoc-17a5407e",
                    "Ipv6CidrBlockState": {
                        "State": "ASSOCIATED"
                    }
                }
            ],
            ...
}
```

3. Crie uma sub-rede com um bloco CIDR IPv4 `10.0.0.0/24` e um bloco CIDR IPv6 `2001:db8:1234:1a00::/64` (dos intervalos que foram retornados na etapa anterior).

```
aws ec2 create-subnet --vpc-id vpc-2f09a348 --cidr-block 10.0.0.0/24 --ipv6-cidr-
block 2001:db8:1234:1a00::/64
```

4. Crie uma segunda sub-rede em sua VPC com um bloco CIDR IPv4 `10.0.1.0/24` e um bloco CIDR IPv6 `2001:db8:1234:1a01::/64`.

```
aws ec2 create-subnet --vpc-id vpc-2f09a348 --cidr-block 10.0.1.0/24 --ipv6-cidr-
block 2001:db8:1234:1a01::/64
```

Etapa 2: Configurar uma sub-rede pública

Assim que criar a VPC e as sub-redes, poderá tornar uma das sub-redes uma sub-rede pública, anexando um gateway da Internet à sua VPC, criando uma tabela de rotas personalizada e configurando o roteamento da sub-rede para o Gateway da internet. Nesse exemplo, uma tabela de rotas é criada e faz o roteamento de todos os tráfegos IPv4 e IPv6 para um gateway da Internet.

Para tornar sua sub-rede uma sub-rede pública

1. Crie um gateway da Internet.

```
aws ec2 create-internet-gateway
```

   Na saída retornada, anote o ID do Internet Gateway.

```
{
    "InternetGateway": {
        ...
        "InternetGatewayId": "igw-1ff7a07b",
        ...
    }
}
```

2. Usando o ID da etapa anterior, anexe o Internet Gateway à sua VPC.

```
aws ec2 attach-internet-gateway --vpc-id vpc-2f09a348 --internet-gateway-
id igw-1ff7a07b
```

3. Crie uma tabela de rotas personalizada para sua VPC.

```
aws ec2 create-route-table --vpc-id vpc-2f09a348
```

Na saída retornada, anote o ID da tabela de rotas.

```
{
    "RouteTable": {
        ...
        "RouteTableId": "rtb-c1c8faa6",
        ...
    }
}
```

4. Crie uma rota na tabela que direcione todo tráfego IPv6 (`::/0`) para o Internet Gateway.

```
aws ec2 create-route --route-table-id rtb-c1c8faa6 --destination-ipv6-cidr-block ::/0
 --gateway-id igw-1ff7a07b
```

> **Note**
>
> Se tiver intenção de usar sua sub-rede público para tráfego IPv4 também, precisará adicionar outra rota para o tráfego `0.0.0.0/0`, direcionada para o Internet Gateway.

5. Para confirmar se a rota foi criada e está ativa, você pode descrever a tabela de rotas e visualizar os resultados.

```
aws ec2 describe-route-tables --route-table-id rtb-c1c8faa6
```

```
{
    "RouteTables": [
        {
            "Associations": [],
            "RouteTableId": "rtb-c1c8faa6",
            "VpcId": "vpc-2f09a348",
            "PropagatingVgws": [],
            "Tags": [],
            "Routes": [
                {
                    "GatewayId": "local",
                    "DestinationCidrBlock": "10.0.0.0/16",
                    "State": "active",
                    "Origin": "CreateRouteTable"
                },
                {
                    "GatewayId": "local",
                    "Origin": "CreateRouteTable",
                    "State": "active",
                    "DestinationIpv6CidrBlock": "2001:db8:1234:1a00::/56"
                },
                {
                    "GatewayId": "igw-1ff7a07b",
                    "Origin": "CreateRoute",
                    "State": "active",
                    "DestinationIpv6CidrBlock": "::/0"
                }
            ]
        }
    ]
}
```

6. No momento, a tabela de rotas não está associada a nenhuma sub-rede. Associe a tabela a uma sub-rede em sua VPC para que o tráfego dessa sub-rede seja roteado para o Internet Gateway. Primeiro, descreva suas sub-redes para obter os IDs. Você pode usar a opção `--filter` para retornar as sub-redes apenas para sua nova VPC e a opção `--query` para retornar somente os IDs de sub-rede e os respectivos blocos CIDR IPv4 e IPv6.

```
aws ec2 describe-subnets --filters "Name=vpc-id,Values=vpc-2f09a348" --query
 'Subnets[*].
{ID:SubnetId,IPv4CIDR:CidrBlock,IPv6CIDR:Ipv6CidrBlockAssociationSet[*].Ipv6CidrBlock}'
```

```
[
    {
        "IPv6CIDR": [
            "2001:db8:1234:1a00::/64"
        ],
        "ID": "subnet-b46032ec",
        "IPv4CIDR": "10.0.0.0/24"
    },
    {
        "IPv6CIDR": [
            "2001:db8:1234:1a01::/64"
        ],
        "ID": "subnet-a46032fc",
        "IPv4CIDR": "10.0.1.0/24"
    }
]
```

7. Você pode escolher com qual sub-rede deseja associar a tabela de rotas personalizada; por exemplo, `subnet-b46032ec`. Essa sub-rede será sua sub-rede pública.

```
aws ec2 associate-route-table  --subnet-id subnet-b46032ec --route-table-id rtb-
c1c8faa6
```

Etapa 3: Configurar uma sub-rede privada apenas de saída

Você pode configurar a segunda sub-rede em sua VPC para ser uma sub-rede privada IPv6 apenas de saída. as instâncias que são executadas nessa sub-rede podem acessar a Internet por IPv6 (por exemplo, para obter atualizações de software) por meio de um Internet Gateway apenas de saída, mas os hosts na Internet não podem acessar suas instâncias.

Para tornar sua sub-rede uma sub-rede privada apenas de saída

1. Crie um gateway da Internet apenas de saída para sua VPC. Na saída retornada, anote o ID do gateway.

```
aws ec2 create-egress-only-internet-gateway --vpc-id vpc-2f09a348
```

```
{
    "EgressOnlyInternetGateway": {
        "EgressOnlyInternetGatewayId": "eigw-015e0e244e24dfe8a",
        "Attachments": [
            {
                "State": "attached",
                "VpcId": "vpc-2f09a348"
            }
```

```
        ]
    }
}
```

2. Crie uma tabela de rotas personalizada para sua VPC. Na saída retornada, anote o ID da tabela de rotas.

```
aws ec2 create-route-table --vpc-id vpc-2f09a348
```

3. Crie uma rota na tabela que direcione todo tráfego IPv6 (`::/0`) para o Internet Gateway apenas de saída.

```
aws ec2 create-route --route-table-id rtb-abc123ab --destination-ipv6-cidr-block ::/0
 --egress-only-internet-gateway-id eigw-015e0e244e24dfe8a
```

4. Associe a tabela de rotas à segunda sub-rede em sua VPC (você descreveu as sub-redes na seção anterior). Essa sub-rede será sua sub-rede privada com acesso IPv6 apenas de saída à Internet.

```
aws ec2 associate-route-table --subnet-id subnet-a46032fc --route-table-id rtb-abc123ab
```

Etapa 4: Modificar o comportamento do endereçamento IPv6 das sub-redes

Você pode modificar o comportamento do endereçamento IP de suas sub-redes para que as instâncias executadas recebam endereços IPv6 automaticamente. Quando você executar uma instância na sub-rede, um único endereço IPv6 do intervalo da sub-rede será atribuído à interface de rede primárias (eth0) da instância.

```
aws ec2 modify-subnet-attribute --subnet-id subnet-b46032ec --assign-ipv6-address-on-
creation
```

```
aws ec2 modify-subnet-attribute --subnet-id subnet-a46032fc --assign-ipv6-address-on-
creation
```

Etapa 5: Executar uma instância na sub-rede pública

Para testar se sua sub-rede pública é pública e se suas instâncias na sub-rede são acessíveis pela Internet, execute uma instância em sua sub-rede pública e conecte-se a ela. Primeiro, você precisa criar um security group para ser associado com sua instância e um par de chaves com o qual você se conectará à sua instância. Para mais informações sobre security groups, consulte Grupos de segurança para a VPC (p. 180). Para obter mais informações sobre pares de chaves, consulte Pares de chaves do Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias do Linux.

Para executar e conectar-se a uma instância em sua sub-rede pública

1. Crie um par de chaves e use a opção `--query` e a opção de texto `--output` para canalizar sua chave privada diretamente em um arquivo com a extensão `.pem`.

```
aws ec2 create-key-pair --key-name MyKeyPair --query 'KeyMaterial' --output text
 > MyKeyPair.pem
```

Neste exemplo, execute uma instância do Amazon Linux. Se você usar um cliente SSH em um sistema operacional Linux ou OS X para se conectar à sua instância, use o seguinte comando para definir as permissões do arquivo de chave privada, de maneira que apenas você possa lê-lo.

```
chmod 400 MyKeyPair.pem
```

2. Crie um security group para sua VPC e adicione uma regra que permita que acesso SSH de qualquer endereço IPv6.

```
aws ec2 create-security-group --group-name SSHAccess --description "Security group for
 SSH access" --vpc-id vpc-2f09a348
```

```
{
    "GroupId": "sg-e1fb8c9a"
}
```

```
aws ec2 authorize-security-group-ingress --group-id sg-e1fb8c9a --ip-permissions
 '[{"IpProtocol": "tcp", "FromPort": 22, "ToPort": 22, "Ipv6Ranges": [{"CidrIpv6":
 "::/0"}]}]'
```

   Note

   Se usar `::/0`, permitirá que todos os endereços IPv6 acessem sua instância usando SSH. Isso é aceitável para esse breve exercício. Porém, na produção, autorize somente um endereço IP específico ou um intervalo de endereços a acessar sua instância.

3. Execute uma instância em sua sub-rede pública, usando o security group e o par de chaves que você criou. Examine o resultado e anote o ID de sua instância.

```
aws ec2 run-instances --image-id ami-0de53d8956e8dcf80 --count 1 --instance-
type t2.micro --key-name MyKeyPair --security-group-ids sg-e1fb8c9a --subnet-id subnet-
b46032ec
```

   Note

   Neste exemplo, a AMI é uma AMI do Amazon Linux na região Leste dos EUA (Norte da Virgínia). Se estiver em uma região diferentes, precisará do ID de uma AMI adequada à sua região. Para obter mais informações, consulte Encontrar uma AMI do Linux no Guia do usuário do Amazon EC2 para instâncias do Linux.

4. Sua instância precisa estar no estado `running` para você se conectar a ela. Descreve sua instância, confirme o estado dela e tome nota do respectivo endereço IPv6.

```
aws ec2 describe-instances --instance-id i-0146854b7443af453
```

```
{
    "Reservations": [
        {
            ...
            "Instances": [
                {
                    ...
                    "State": {
                        "Code": 16,
                        "Name": "running"
                    },
```

```
                    ...
                    "NetworkInterfaces": {
                        "Ipv6Addresses": {
                            "Ipv6Address": "2001:db8:1234:1a00::123"
                        }
                    ...
                }
            ]
        }
    ]
}
```

5. Quando sua instância se encontra no estado de execução, você pode conectar-se a ela usando um cliente SSH em um computador Linux ou OS X por meio do comando a seguir. Seu computador local precisa estar configurado para um endereço IPv6.

```
ssh -i "MyKeyPair.pem" ec2-user@2001:db8:1234:1a00::123
```

   Se você estiver se conectando de um computador Windows, use as instruções a seguir: Conectar-se à instância do Linux no Windows utilizando PuTTY.

Etapa 6: Executar uma instância na sub-rede privada

Para testar se as instâncias em sua sub-rede privada apenas de saída conseguem acessar a Internet, execute uma instância em sua sub-rede privada e conecte-se a ela usando uma instância bastion em sua sub-rede pública (você pode usar a instância que executou na seção anterior). Primeiro, você precisa criar um security group para a instância. O security group precisa ter uma regra que permita que sua instância bastion conecte-se usando SSH e uma regra que permita que o comando `ping6` (tráfego ICMPv6) verifique se a instância não pode ser acessada pela Internet.

1. Crie um security group em sua VPC e adicione uma regra que permita acesso SSH de entrada do endereço IPv6 da instância em sua sub-rede pública e uma regra que permita todo o tráfego ICMPv6:

```
aws ec2 create-security-group --group-name SSHAccessRestricted --description "Security
 group for SSH access from bastion" --vpc-id vpc-2f09a348
```

```
{
    "GroupId": "sg-aabb1122"
}
```

```
aws ec2 authorize-security-group-ingress --group-id sg-aabb1122 --ip-permissions
 '[{"IpProtocol": "tcp", "FromPort": 22, "ToPort": 22, "Ipv6Ranges": [{"CidrIpv6":
 "2001:db8:1234:1a00::123/128"}]}]'
```

```
aws ec2 authorize-security-group-ingress --group-id sg-aabb1122 --ip-permissions
 '[{"IpProtocol": "58", "FromPort": -1, "ToPort": -1, "Ipv6Ranges": [{"CidrIpv6":
 "::/0"}]}]'
```

2. Execute uma instância em sua sub-rede privada, usando o security group que você criou e o mesmo par de chaves usado para executar a instância na sub-rede pública.

```
aws ec2 run-instances --image-id ami-a4827dc9 --count 1 --instance-type t2.micro --key-
name MyKeyPair --security-group-ids sg-aabb1122 --subnet-id subnet-a46032fc
```

Use o comando `describe-instances` para verificar se sua instância está em execução e para obter o respectivo endereço IPv6.

3. Configure o encaminhamento de agente SSH em seu computador local e conecte-se à sua instância na sub-rede pública. Para o Linux, use os comandos a seguir:

```
ssh-add MyKeyPair.pem
```

```
ssh -A ec2-user@2001:db8:1234:1a00::123
```

Para o OS X, use os comandos a seguir:

```
ssh-add -K MyKeyPair.pem
```

```
ssh -A ec2-user@2001:db8:1234:1a00::123
```

Para o Windows, use as instruções a seguir: Para configurar o encaminhamento de agente SSH para Windows (PuTTY) (p. 234). Conecte-se à instância na sub-rede pública usando o respectivo endereço IPv6.

4. Em sua instância na sub-rede pública (a instância bastion), conecte-se à sua instância na sub-rede privada usando o respectivo endereço IPv6:

```
ssh ec2-user@2001:db8:1234:1a01::456
```

5. Na instância privada, teste se é possível conectar-se à internet executando o comando `ping6` para um site que tenha o ICMP habilitado, por exemplo:

```
ping6 -n ietf.org
```

```
PING ietf.org(2001:1900:3001:11::2c) 56 data bytes
64 bytes from 2001:1900:3001:11::2c: icmp_seq=1 ttl=46 time=73.9 ms
64 bytes from 2001:1900:3001:11::2c: icmp_seq=2 ttl=46 time=73.8 ms
64 bytes from 2001:1900:3001:11::2c: icmp_seq=3 ttl=46 time=73.9 ms
...
```

6. Para testar se os hosts na Internet não conseguem acessar sua instância na sub-rede privada, use o comando `ping6` em um computador habilitado para IPv6. Você deve obter uma resposta de tempo limite. Se você obtiver uma resposta válida, isso significa que a instância pode ser acessada pela Internet: verifique a tabela de rotas associada à sub-rede privada e confirme se ela não contém uma rota que direciona o tráfego IPv6 para um gateway da Internet.

```
ping6 2001:db8:1234:1a01::456
```

Etapa 7: Limpeza

Assim que verificar se você consegue conectar-se à sua instância na sub-rede pública e se sua instância na sub-rede pública consegue acessar a Internet, poderá encerrar as instâncias se não precisar mais delas. Para isso, use o comando terminate-instances. Par excluir os outros recursos que você criou neste exemplo, use os comandos a seguir na ordem em que são listados:

1. Exclua seus security groups:

```
aws ec2 delete-security-group --group-id sg-e1fb8c9a
```

```
aws ec2 delete-security-group --group-id sg-aabb1122
```

2. Exclua suas sub-redes:

```
aws ec2 delete-subnet --subnet-id subnet-b46032ec
```

```
aws ec2 delete-subnet --subnet-id subnet-a46032fc
```

3. Exclua suas tabelas de rotas personalizadas:

```
aws ec2 delete-route-table --route-table-id rtb-c1c8faa6
```

```
aws ec2 delete-route-table --route-table-id rtb-abc123ab
```

4. Exclua o Internet Gateway da VPC:

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-1ff7a07b --vpc-id vpc-2f09a348
```

5. Exclua seu Internet Gateway:

```
aws ec2 delete-internet-gateway --internet-gateway-id igw-1ff7a07b
```

6. Exclua seu Internet Gateway apenas de saída:

```
aws ec2 delete-egress-only-internet-gateway  --egress-only-internet-gateway-
id eigw-015e0e244e24dfe8a
```

7. Exclua sua VPC:

```
aws ec2 delete-vpc --vpc-id vpc-2f09a348
```

VPCs e sub-redes

Para começar a usar a Amazon Virtual Private Cloud (Amazon VPC), crie uma VPC e sub-redes. Para obter uma visão geral da Amazon VPC, consulte O que é Amazon VPC? (p. 1).

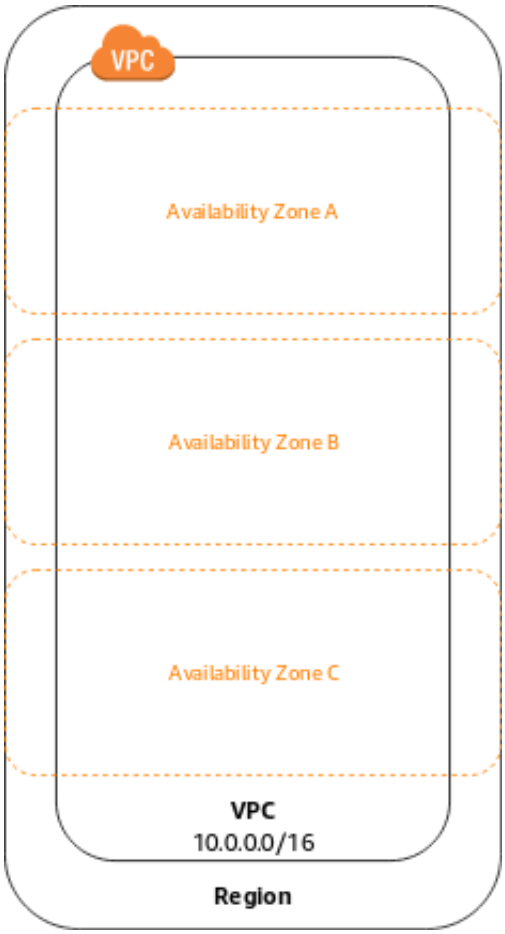
Tópicos

Conceitos básicos de sub-rede e VPC

Uma virtual private cloud (VPC) é uma rede virtual dedicada a sua conta da AWS Ela é isolada de maneira lógica das outras redes virtuais na Nuvem AWS. É possível executar os recursos da AWS, como instâncias do Amazon EC2, na VPC.

Quando você cria uma VPC, é necessário especificar um intervalo de endereços IPv4 para a VPC sob a forma de um bloco CIDR (Roteamento entre Domínios sem Classificação); por exemplo, `10.0.0.0/16`. Este é o bloco CIDR principal da VPC. Para obter mais informações sobre notação CIDR, consulte RFC 4632.

O diagrama a seguir mostra uma nova VPC com um bloco CIDR IPv4.



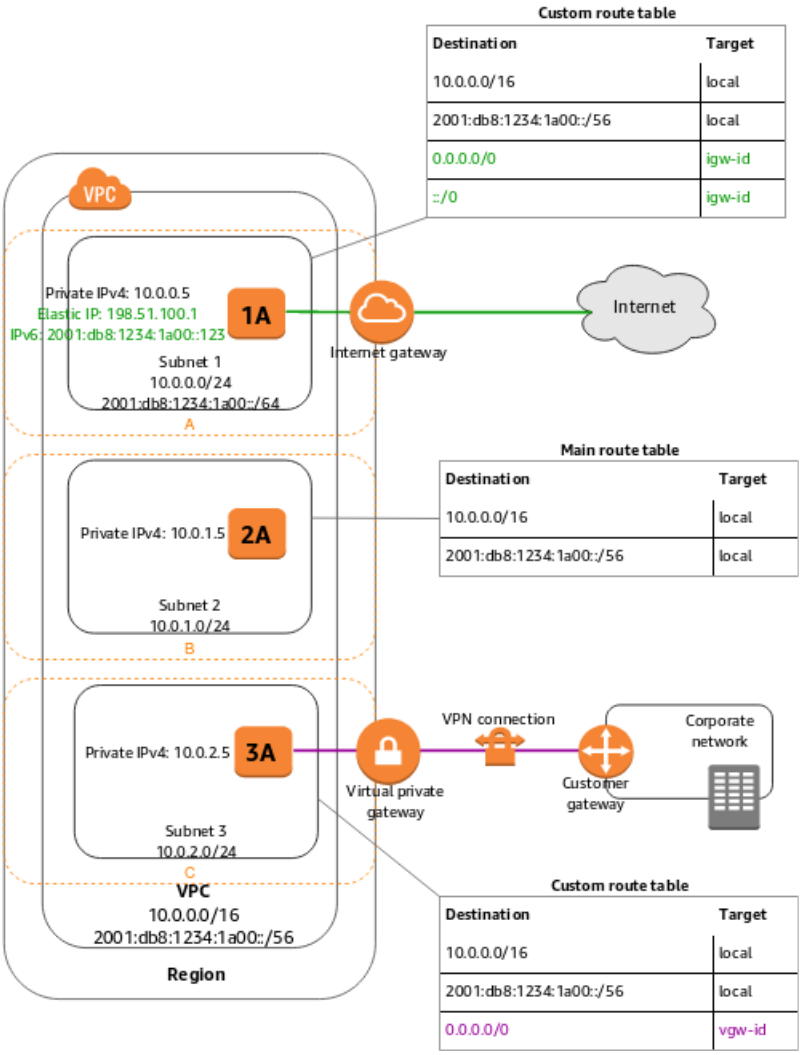
A tabela de rotas principais tem as rotas a seguir.

Destino	Destino
10.0.0.0/16	local

Uma VPC abrange todas as zonas de disponibilidade na região. Depois de criar uma VPC, você pode adicionar uma ou mais sub-redes em cada zona de disponibilidade. Também é possível adicionar sub-redes em uma zona local, que é uma implantação de infraestrutura da AWS que coloca computação, armazenamento, banco de dados e outros serviços selecionados mais próximos de seus usuários finais. Uma zona local permite que os usuários finais executem aplicativos que exigem latências de milissegundos de um dígito. Para obter informações sobre as regiões que oferecem suporte a zonas locais, consulte Regiões disponíveis no Guia do usuário do Amazon EC2 para instâncias do Linux. Ao criar uma sub-rede, você especifica o bloco CIDR para a sub-rede, que é um subconjunto do bloco CIDR da VPC. Cada sub-rede deve residir inteiramente dentro de uma zona de disponibilidade e não pode abranger áreas. As zonas de disponibilidade são locais distintos que são projetados para serem isolados de falhas em outras zonas de disponibilidade. Ao iniciar as instâncias em Zonas de disponibilidade separadas, você pode proteger seus aplicativos de falha de um único local. Nós atribuímos um ID exclusivo a cada sub-rede.

Você também pode atribuir opcionalmente um bloco CIDR IPv6 a sua VPC e atribuir blocos CIDR IPv6 às suas sub-redes.

O diagrama a seguir mostra uma VPC que foi configurada com sub-redes em várias zonas de disponibilidade. 1A, 2A e 3A são instâncias na sua VPC. Um bloco CIDR IPv6 está associada à VPC e um bloco CIDR IPv6 está associado à sub-rede 1. Um gateway da internet permite comunicação através da Internet, e uma conexão de rede privada virtual (VPN) permite comunicação com a rede corporativa.



Se o tráfego de uma sub-rede for roteado para um gateway da internet, a sub-rede será conhecida como uma sub-rede pública. Neste diagrama, a sub-rede 1 é uma sub-rede pública. Se você desejar que a instância em uma sub-rede pública se comunique com a internet por meio do IPv4, ela deve ter um endereço IPv4 público ou um endereço IP elástico (IPv4). Para mais informações sobre endereços IPv4 públicos, consulte Endereços IPv4 públicos (p. 119). Se você desejar que a instância na sub-rede pública se comunique com a internet por meio do IPv6, ela deverá ter um endereço IPv6.

Se uma sub-rede não tiver uma rota para o gateway da internet, a sub-rede será conhecida como uma sub-rede privada. Neste diagrama, a sub-rede 2 é uma sub-rede privada.

Se uma sub-rede não tiver uma rota para o gateway da internet, mas tiver seu tráfego roteado para um gateway privado virtual de uma conexão Site-to-Site VPN, a sub-rede será conhecida como uma sub-rede somente VPN. Neste diagrama, a sub-rede 3 é uma sub-rede somente VPN. Atualmente, não oferecemos suporte para tráfego IPv6 em conexão Site-to-Site VPN.

Para mais informações, consulte Exemplos para a VPC (p. 80), Gateways da Internet (p. 212) e O que é o AWS Site-to-Site VPN? no Guia do usuário do AWS Site-to-Site VPN.

> **Note**
>
> Independentemente do tipo de sub-rede, o intervalo de endereços IPv4 interno da sub-rede é sempre privado: não anunciamos o bloco de endereços para a Internet.

Você tem uma cota no número de VPCs e sub-redes que pode criar em sua conta. Para obter mais informações, consulte Cotas da Amazon VPC (p. 345).

Dimensionamento da VPC e da sub-rede

A Amazon VPC oferece suporte ao endereçamento de IPv4 e IPv6 e tem diferentes cotas de tamanho de bloco CIDR para cada um. Por padrão, todos as VPCs e as sub-redes devem ter blocos CIDR IPv4 — você não pode alterar este comportamento. Opcionalmente, você pode associar um bloco CIDR IPv6 à VPC.

Para obter mais informações sobre endereçamento IP, consulte Endereçamento IP na sua VPC (p. 117).

Tópicos

Dimensionamento da VPC e da sub-rede para IPv4

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 secundários à VPC. Para obter mais informações, consulte Adicionar blocos CIDR IPv4 a uma VPC (p. 104).

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)	A VPC deve ser /16 ou menor, por exemplo, `10.0.0.0/16`.
`172.16.0.0` - `172.31.255.255` (prefixo 172.16/12)	A VPC deve ser /16 ou menor, por exemplo, `172.31.0.0/16`.
`192.168.0.0` - `192.168.255.255` (prefixo 192.168/16)	A VPC pode ser menor, por exemplo `192.168.0.0/20`.

Você pode criar uma VPC com um bloco CIDR roteável publicamente que fica fora dos intervalos de endereços IPv4 privados especificados no RFC 1918. No entanto, para os fins desta documentação, nos referimos a endereços IP privados como os endereços IPv4 que estão dentro do intervalo CIDR da sua VPC.

> **Note**
>
> Se estiver criando uma VPC para uso com outro serviço da AWS, verifique a documentação do serviço para verificar se há requisitos específicos para o intervalo de endereços IP ou os componentes da rede.

O bloco CIDR de uma sub-rede pode ser igual ao bloco CIDR para a VPC (para uma única sub-rede na VPC) ou um subconjunto do bloco CIDR para a VPC (para várias sub-redes). O tamanho do bloco permitido é entre uma máscara de rede `/28` e máscara de rede `/16`. 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 disponíveis na Internet para ajudar a calcular e criar blocos CIDR de sub-rede IPv4; por exemplo, IPv4 Address Planner. É possível encontrar outras ferramentas que se adequam às suas necessidades procurando termos como “calculadora de sub-rede” ou “calculadora de CIDR”. O grupo de engenharia de rede também pode ajudar a determinar os blocos CIDR para especificar as sub-redes.

Os primeiros quatro 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 uma instância. 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 DNS é a base do intervalo de rede da VPC mais dois. Para VPCs com vários blocos CIDR, o endereço IP de servidor 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 obter mais informações, consulte Servidor DNS da Amazon (p. 258).
- `10.0.0.3`: reservado pela AWS para uso futuro.
- `10.0.0.255`: endereço de transmissão de rede. Nós não oferecemos suporte para transmissão em uma VPC, portanto, nós reservamos este endereço.

Se você criar uma VPC ou uma sub-rede usando uma ferramenta de 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`.

Adicionar blocos CIDR IPv4 a 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 à esquerda tem um único bloco CIDR (`10.0.0.0/16`) e duas sub-redes. A VPC à direita representa a arquitetura da mesma VPC depois de você adicionar um segundo bloco CIDR (`10.2.0.0/16`) e criar uma nova sub-rede no intervalo do segundo CIDR.

Destination	Target
10.0.0.0/16	local

Destination	Target
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 (p. 106).
- Você não pode 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 (p. 345).
- 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.

- Se tiver habilitado a VPC para o ClassicLink, você poderá associar blocos CIDR nos intervalos `10.1.0.0/16` e `10.0.0.0/16`, mas não poderá associar nenhum outro bloco CIDR no intervalo `10.0.0.0/8`.
- 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 de 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 de 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 de 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 de 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 Guia 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`.

A tabela a seguir fornece uma visão geral das associações de bloco CIDR permitidas e restritas que dependem do intervalo de endereços IPv4 no qual o bloco CIDR principal da VPC reside.

Restrições de associação de bloco CIDR IPv4

Intervalo de endereços IP no qual o bloco CIDR principal da VPC reside	Associações de bloco CIDR restritas	Associações de bloco CIDR 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 o CIDR principal estiver no intervalo 10.0.0.0/15, você não poderá adicionar um bloco CIDR no intervalo 10.0.0.0/16. Um bloco CIDR no intervalo 198.19.0.0/16.	Qualquer outro CIDR no intervalo 10.0.0.0/8 que não seja restrito. Qualquer bloco CIDR IPv4 publicamente roteável (não RFC 1918) ou um bloco CIDR da faixa 100.64.0.0/10.
172.16.0.0/12	Blocos CIDR de outros intervalos RFC 1918* (10.0.0.0/8 e 192.168.0.0/16). Um bloco CIDR no intervalo 172.31.0.0/16.	Qualquer outro CIDR no intervalo 172.16.0.0/12 que não seja restrito. Qualquer bloco CIDR IPv4 publicamente roteável (não RFC 1918) ou um bloco CIDR da faixa 100.64.0.0/10.

Intervalo de endereços IP no qual o bloco CIDR principal da VPC reside	Associações de bloco CIDR restritas	Associações de bloco CIDR permitidas
	Um bloco CIDR no intervalo 198.19.0.0/16.	
192.168.0.0/16	Blocos CIDR de outros intervalos RFC 1918* (172.16.0.0/12 e 10.0.0.0/8). Um bloco CIDR no intervalo 198.19.0.0/16.	Qualquer outro CIDR no intervalo 192.168.0.0/16. Qualquer bloco CIDR IPv4 publicamente roteável (não RFC 1918) ou um bloco CIDR da faixa 100.64.0.0/10.
198.19.0.0/16	Blocos CIDR nos intervalos RFC 1918*.	Qualquer bloco CIDR IPv4 publicamente roteável (não RFC 1918) ou um bloco CIDR da faixa 100.64.0.0/10.
Bloco CIDR publicamente roteável (não RFC 1918) ou um bloco CIDR da faixa 100.64.0.0/10.	Blocos CIDR nos intervalos RFC 1918*. Um bloco CIDR no intervalo 198.19.0.0/16.	Qualquer outro bloco CIDR IPv4 publicamente roteável (não RFC 1918) ou um bloco CIDR da faixa 100.64.0.0/10.

Os intervalos *RFC 1918 são os intervalos de endereços IPv4 privados especificados na RFC 1918.

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 principal da VPC no console da Amazon VPC, escolha Your VPCs (Suas VPCs), selecione a VPC e anote a primeira entrada em CIDR blocks (Blocos CIDR). Como alternativa, use o comando describe-vpcs:

```
aws ec2 describe-vpcs --vpc-id vpc-1a2b3c4d
```

Na saída retornada, o CIDR principal é retornado no elemento `CidrBlock` de nível superior (o penúltimo elemento na saída do exemplo a seguir).

```
{
    "Vpcs": [
        {
            "VpcId": "vpc-1a2b3c4d",
            "InstanceTenancy": "default",
            "Tags": [
                {
                    "Value": "MyVPC",
                    "Key": "Name"
                }
            ],
            "CidrBlockAssociations": [
                {
                    "AssociationId": "vpc-cidr-assoc-3781aa5e",
                    "CidrBlock": "10.0.0.0/16",
                    "CidrBlockState": {
                        "State": "associated"
                    }
                },
                {
                    "AssociationId": "vpc-cidr-assoc-0280ab6b",
```

```
                    "CidrBlock": "10.2.0.0/16",
                    "CidrBlockState": {
                        "State": "associated"
                    }
                }
            ],
            "State": "available",
            "DhcpOptionsId": "dopt-e0fe0e88",
            "CidrBlock": "10.0.0.0/16",
            "IsDefault": false
        }
    ]
}
```

Dimensionamento da VPC e da sub-rede para IPv6

Você pode associar um único bloco CIDR IPv6 com uma VPC existente em sua conta ou ao criar uma nova VPC. O bloco CIDR é um comprimento de prefixo fixo de `/56`. É possível solicitar um bloco CIDR IPv6 do grupo de endereços IPv6 da Amazon.

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. O bloco CIDR IPv6 de uma sub-rede é um comprimento de prefixo fixo de `/64`.

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`.

Existem ferramentas disponíveis na Internet para ajudar a calcular e criar blocos CIDR de sub-rede IPv6; por exemplo, IPv6 Address Planner. 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.

Você pode desassociar um bloco CIDR IPv6 de uma sub-rede e você pode 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.

Os primeiros quatro 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. 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`
- `2001:db8:1234:1a00::2`
- `2001:db8:1234:1a00::3`
- `2001:db8:1234:1a00:ffff:ffff:ffff:ffff`

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 obter mais informações, consulte Tabelas de rotas para sua VPC (p. 283).

No diagrama anterior, a tabela de rotas associada à sub-rede 1 roteia todo o tráfego IPv4 (`0.0.0.0/0`) e o tráfego IPv6 (`::/0`) para um gateway da internet (por exemplo, `igw-1a2b3c4d`). Como a instância 1A tem um endereço IP elástico IPv4 e um endereço IPv6, ela pode ser acessada pela Internet por IPv4 e IPv6.

> Note
>
> (Somente IPv4) O endereço IPv4 elástico ou o endereço IPv4 público que está associado à instância é acessado pelo gateway da internet da VPC. O tráfego que passa por uma conexão AWS Site-to-Site VPN entre a instância e outra rede atravessa um gateway privado virtual, não o gateway da Internet, e, portanto, não acessa o endereço IPv4 elástico ou o endereço IPv4 público.

A instância 2A não pode acessar a internet, mas pode acessar outras instâncias na VPC. Você pode permitir que uma instância na VPC inicie conexões de saída para a internet por meio do IPv4, mas evite conexões de entrada não solicitadas da internet usando um gateway de conversão de endereço de rede (NAT) ou uma instância. Como você pode alocar um número limitado de endereços IP elásticos, recomendamos que você use um dispositivo NAT caso tenha mais instâncias que exigem um endereço IP público estático. Para obter mais informações, consulte Dispositivos NAT para sua VPC (p. 228). Para iniciar a comunicação somente de saída com a Internet por meio do IPv6, você pode usar um gateway da internet somente de saída. Para obter mais informações, consulte Gateways da Internet apenas de saída (p. 218).

A tabela de rotas associada à sub-rede 3 roteia todo o tráfego IPv4 (`0.0.0.0/0`) para um gateway privado virtual (por exemplo, `vgw-1a2b3c4d`). A instância 3A pode chegar a computadores na rede corporativa pela conexão Site-to-Site VPN.

Segurança de sub-rede

A AWS fornece dois recursos que você pode usar para aumentar a segurança da VPC: grupos de segurança e ACLs da rede. Os grupos de segurança controlam o tráfego de entrada e de saída de suas instâncias e as Network ACL controlam o tráfego de entrada e de saída de suas sub-redes. Na maioria dos casos, os grupos de segurança podem atender as suas necessidades; contudo, você também pode usar as Network ACL se desejar uma camada adicional de segurança para o seu VPC. Para obter mais informações, consulte Privacidade do tráfego entre redes na Amazon VPC (p. 158).

Por design, cada sub-rede deve estar associada a um Network ACL. Toda sub-rede que você cria está automaticamente associada ao Network ACL padrão da VPC. Você pode alterar a associação e o conteúdo do Network ACL padrão. Para obter mais informações, consulte Network ACLs (p. 190).

Você pode criar um registro 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 registro de fluxo em uma interface de rede individual. Os logs de fluxo são publicados no CloudWatch Logs ou no Amazon S3. Para obter mais informações, consulte VPC Flow Logs (p. 310).

Trabalhar com VPCs e sub-redes

Os seguintes procedimentos são para criar manualmente uma VPC e sub-redes. Você também deve adicionar manualmente gateways e tabelas de roteamento. Como alternativa, é possível usar o assistente da Amazon VPC para criar uma VPC e suas sub-redes, gateways e tabelas de roteamento em uma etapa. Para obter mais informações, consulte Exemplos para a VPC (p. 80).

Tarefas

Criar uma VPC

É possível criar uma VPC vazia usando o console da Amazon VPC.

Para criar 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), Create VPC (Criar VPC).
3. Especifique os seguintes detalhes da VPC conforme necessário.

   - Name tag (Tag do nome): opcionalmente, forneça um nome para a sua VPC. Ao fazer isso, é criada uma tag com a chave `Name` e o valor especificado.
   - Bloco CIDR IPv4: Especifique um bloco CIDR IPv4 para sua VPC. O menor bloco CIDR que pode ser especificado é /28 e o maior é /16. Recomendamos que você especifique um bloco CIDR a partir dos intervalos de endereços IP privados (não roteados publicamente) conforme especificado em RFC 1918; por exemplo, `10.0.0.0/16` ou `192.168.0.0/16`.

     Note

     É possível especificar um intervalo de endereços IPv4 publicamente roteáveis. No entanto, atualmente não oferecemos suporte para acesso direto à Internet de blocos CIDR publicamente roteáveis em uma VPC. As instâncias do Windows não podem inicializar corretamente se forem executadas em uma VPC com intervalos de `224.0.0.0` a `255.255.255.255` (intervalos de endereço IP de classe D e classe E).
   - IPv6 CIDR block (Bloco CIDR IPv6): é possível associar um bloco CIDR IPv6 à VPC. Escolha uma das seguintes opções e selecione Select CIDR (Selecionar CIDR):
     - Amazon-provided IPv6 CIDR block (Bloco CIDR IPv6 fornecido pela Amazon): solicita 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.
     - IPv6 CIDR owned by me (CIDR IPv6 pertencente a mim): (BYOIP) aloca um bloco CIDR IPv6 do seu grupo de endereços IPv6. Para Pool (Grupo), escolha o grupo de endereços IPv6 a partir do qual alocar o bloco CIDR IPv6.
   - Tenancy (Locação): Selecionar uma opção de locação. Locação dedicada garante que suas instâncias sejam executadas em um hardware com locação única. Para obter mais informações, consulte Instâncias dedicadas no Guia do usuário do Amazon EC2 para instâncias do Linux.
   - (Opcional) Adicione ou remova uma tag.

     [Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

     - Em Key (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.

4. Escolha Create (Criar).

Como alternativa, você pode usar uma ferramenta de linha de comando.

Para criar uma VPC usando uma ferramenta de linha de comando

- create-vpc (CLI da AWS)
- New-EC2Vpc (AWS Tools for Windows PowerShell)

Para descrever uma VPC usando uma ferramenta de linha de comando

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

Para obter mais informações sobre endereços IP, consulte Endereçamento IP na sua VPC (p. 117).

Depois de criar uma VPC, você pode criar sub-redes. Para obter mais informações, consulte Criar uma sub-rede na VPC (p. 111).

Criar uma sub-rede na VPC

Para adicionar uma nova sub-rede à VPC, você deve especificar um bloco CIDR IPv4 para a sub-rede no intervalo da VPC. Você pode especificar a zona de disponibilidade na qual você deseja que a sub-rede resida. Você pode ter várias sub-redes em uma mesma zona de disponibilidade.

Você poderá, opcionalmente, especificar um bloco CIDR IPv6 para sua sub-rede se um bloco CIDR IPv6 estiver associado a sua VPC.

Para criar a sub-rede em uma zona local ou uma zona do Wavelength, é necessário habilitar a zona. Para obter informações sobre como habilitar zonas do Wavelength, consulte Habilitar zonas no Guia do usuário do Amazon EC2 para instâncias do Linux.

Como adicionar uma sub-rede à VPC usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Subnets (Sub-redes), Create Subnet (Criar sub-rede).
3. Especifique os detalhes da sub-rede conforme necessário e escolha Create Subnet (Criar sub-rede).
   - Name tag (Tag de nome): opcionalmente, forneça um nome para sua sub-rede. Ao fazer isso, é criada uma tag com a chave `Name` e o valor especificado.
   - VPC: Escolha a VPC na qual você está criando a sub-rede.
   - Availability Zone (Zona de disponibilidade): é possível escolher uma zona na qual a sub-rede residirá ou deixar o padrão No Preference (Sem preferência) para permitir que a AWS escolha uma zona de disponibilidade para você.

     Para obter informações sobre regiões e zonas, consulte Regiões e zonas no Guia do usuário do Amazon EC2 para instâncias do Linux.
   - Bloco CIDR IPv4: Especifique um bloco CIDR IPv4 para sua sub-rede, por exemplo, `10.0.1.0/24`. Para obter mais informações, consulte Dimensionamento da VPC e da sub-rede para IPv4 (p. 103).

- Bloco CIDR IPv6: (Opcional) Se você associou um bloco CIDR IPv6 a sua VPC, selecione Especificar um CIDR IPv6 personalizado. Especifique o valor do par hexadecimal para a sub-rede ou mantenha o valor padrão.

4. (Opcional) Se necessário, repita as etapas acima para criar mais sub-redes na sua VPC.

Como alternativa, você pode usar uma ferramenta de linha de comando.

Para adicionar uma sub-rede usando uma ferramenta de linha de comando

- create-subnet (CLI da AWS)
- New-EC2Subnet (AWS Tools for Windows PowerShell)

Depois de criar uma sub-rede, você pode fazer o seguinte:

- Configure seu roteamento. Para tornar a sub-rede em uma sub-rede pública, primeiro você deve associar um gateway da internet à VPC. Para obter mais informações, consulte Criar e associar de um gateway da Internet (p. 215). Em seguida, você pode criar uma tabela de rotas personalizada e adicionar uma rota ao gateway da internet. Para obter mais informações, consulte Criar uma tabela de rotas personalizada (p. 216). Para obter outras opções de roteamento, consulte Tabelas de rotas para sua VPC (p. 283).
- Modifique as configurações da sub-rede para especificar que todas as instâncias iniciadas nessa sub-rede recebem um endereço IPv4 público, um endereço IPv6 ou ambos. Para obter mais informações, consulte Comportamento do endereçamento IP para a sub-rede (p. 121).
- Crie ou modifique seus grupos de segurança conforme necessário. Para obter mais informações, consulte Grupos de segurança para a VPC (p. 180).
- Crie ou modifique suas Network ACLs conforme necessário. Para obter mais informações, consulte Network ACLs (p. 190).
- Compartilhe a sub-rede com outras contas. Para obter mais informações, consulte ??? (p. 139).

Visualizar as sub-redes

Você vê os detalhes sobre sua sub-rede.

Para visualizar os detalhes da 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 (Sub-redes).
3. Selecione a sub-rede e, em seguida, escolha View Details.

Para descrever uma sub-rede usando uma ferramenta de linha de comando

- describe-subnets (CLI da AWS)
- Get-EC2Subnet (AWS Tools for Windows PowerShell)

Associar um bloco CIDR IPv4 secundário à VPC

Você pode adicionar outro bloco CIDR IPv4 à VPC. Não deixe de ler as restrições (p. 104) aplicáveis.

Depois de associar um bloco CIDR, o status muda para `associating`. O bloco CIDR está pronto para uso quando estiver no estado `associated`.

O console da Amazon VPC fornece o status da solicitação na parte superior da página.

Para adicionar um bloco CIDR à VPC usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Your VPCs (Suas VPCs).
3. Selecione a VPC e escolha Actions, Edit CIDRs.
4. Escolha Add IPv4 CIDR e digite o bloco CIDR a ser adicionado, por exemplo, `10.2.0.0/16`. Escolha o ícone de tique
5. Escolha Fechar.

Como alternativa, você pode usar uma ferramenta de linha de comando.

Para adicionar um bloco CIDR usando uma ferramenta de linha de comando

- associate-vpc-cidr-block (CLI da AWS)
- Register-EC2VpcCidrBlock (AWS Tools for Windows PowerShell)

Depois de adicionar os blocos CIDR IPv4 necessários, você pode criar sub-redes. Para obter mais informações, consulte Criar uma sub-rede na VPC (p. 111).

Associar um bloco CIDR IPv6 à sua VPC

Você pode associar um bloco CIDR IPv6 a qualquer VPC existente. A VPC não deve ter um bloco CIDR IPv6 existente associado a ela.

Para associar um bloco CIDR IPv6 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, selecione Your VPCs (Suas VPCs).
3. Selecione sua VPC, escolha Ações, Edit CIDRs.
4. Escolha Adicionar CIDR IPv6.
5. Escolha Adicionar CIDR IPv6.
6. Em IPv6 CIDR block (Bloco CIDR IPv6), escolha uma das opções a seguir e selecione Select CIDR (Escolher CIDR):
   - Amazon-provided IPv6 CIDR block (Bloco CIDR IPv6 fornecido pela Amazon): solicita um bloco CIDR IPv6 do grupo de endereços IPv6 da Amazon.
   - IPv6 CIDR owned by me (CIDR IPv6 pertencente a mim): (BYOIP) aloca um bloco CIDR IPv6 do grupo de endereços IPv6. Para Pool (Grupo), escolha o grupo de endereços IPv6 a partir do qual alocar o bloco CIDR IPv6.
7. Se você selecionou Amazon-provided IPv6 CIDR block (Bloco CIDR IPv6 fornecido pela Amazon), em Network Border Group (Grupo de borda de rede), selecione o grupo de onde a AWS anuncia os endereços IP.
8. Escolha Select CIDR (Selecionar CIDR).
9. Escolha Fechar.

Como alternativa, você pode usar uma ferramenta de linha de comando.

Para associar um bloco CIDR IPv6 a uma VPC usando uma ferramenta de linha de comando

- associate-vpc-cidr-block (CLI da AWS)

- Register-EC2VpcCidrBlock (AWS Tools for Windows PowerShell)

Associar um bloco CIDR IPv6 à 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.

Para associar um bloco CIDR IPv6 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 sua sub-rede e escolha Ações de sub-redes, Edit CIDRs IPv6.
4. Escolha Adicionar CIDR IPv6. Especifique o par hexadecimal para a sub-rede (por exemplo, `00`) e confirme a entrada escolhendo o ícone de seleção.
5. Escolha Fechar.

Como alternativa, você pode usar uma ferramenta de linha de comando.

Para associar um bloco CIDR IPv6 a uma sub-rede usando uma ferramenta de linha de comando

- associate-subnet-cidr-block (CLI da AWS)
- Register-EC2SubnetCidrBlock (AWS Tools for Windows PowerShell)

Executar uma instância na sub-rede

Depois de criar a sub-rede e configurar o roteamento, inicie uma instância em sua sub-rede usando o console do Amazon EC2.

Para executar uma instância na sub-rede. usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel, escolha Launch Instance (Executar instância).
3. Siga as orientações no assistente. Selecione um AMI e um tipo de instância e selecione Next: Configure Instance Details (Próximo: configurar detalhes da instância).

   Note

   Se você quiser que sua instância se comunique pelo IPv6, será necessário selecionar um tipo de instância compatível. Todos os tipos de instância da geração atual são compatíveis com endereços IPv6.
4. Na página Configure Instance Details, certifique-se de ter selecionado a VPC necessária na lista Rede e, em seguida, selecione a sub-rede na qual a instância será iniciada. Mantenha as outras configurações padrão nesta página e selecione Next: Add Storage.
5. Nas próximas páginas do assistente, você pode configurar o armazenamento para sua instância e adicionar tags. Na página Configure Security Group, escolha qualquer security group existente que você possui ou siga as instruções do assistente para criar um novo security group. Selecione Review and Launch ao concluir.
6. Revise suas configurações e selecione Iniciar.
7. Selecione um par de chaves existente que você possui ou crie um novo e selecione Iniciar instâncias ao concluir.

Como alternativa, você pode usar uma ferramenta de linha de comando.

Para executar uma instância na sub-rede. usando uma ferramenta de linha de comando

- run-instances (CLI da AWS)
- New-EC2Instance (AWS Tools for Windows PowerShell)

Excluir a sub-rede

Se você não precisa mais de sua sub-rede, é possível excluí-la. Você deve encerrar primeiro quaisquer instâncias na sub-rede.

Para excluir a sub-rede usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Encerre todas as instâncias na sub-rede. Para obter mais informações, consulte Encerrar a instância no Guia do usuário do EC2.
3. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
4. No painel de navegação, escolha Subnets (Sub-redes).
5. Selecione a sub-rede para excluir e selecione Actions (Ações), Delete subnet (Excluir sub-rede).
6. Na caixa de diálogo Delete subnet (Excluir sub-rede), escolha Delete subnet (Excluir sub-rede).

Como alternativa, você pode usar uma ferramenta de linha de comando.

Para excluir uma sub-rede usando uma ferramenta de linha de comando

- delete-subnet (CLI da AWS)
- Remove-EC2Subnet (AWS Tools for Windows PowerShell)

Desassociar um bloco CIDR IPv4 da VPC

Se a VPC tiver mais de um bloco CIDR IPv4 associado a ela, você poderá desassociar um bloco CIDR IPv4 da VPC. Você não pode desassociar o bloco CIDR IPv4 principal. Você só pode desassociar um bloco CIDR inteiro. Não é possível desassociar um subconjunto de um bloco CIDR ou um intervalo mesclado de blocos CIDR. Você deve primeiro excluir todas as sub-redes no bloco CIDR.

Para 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, selecione Your VPCs (Suas VPCs).
3. Selecione a VPC e escolha Actions, Edit CIDRs.
4. Em VPC IPv4 CIDRs, escolha o botão de exclusão (uma cruz) do bloco CIDR a ser removido.
5. Escolha Fechar.

Como alternativa, você pode usar uma ferramenta de linha de comando.

Para remover um bloco CIDR IPv4 de uma VPC usando uma ferramenta de linha de comando

- disassociate-vpc-cidr-block (CLI da AWS)
- Unregister-EC2VpcCidrBlock (AWS Tools for Windows PowerShell)

Desassociar um bloco CIDR IPv6 da sua VPC ou sub-rede

Se você não quiser mais suporte ao IPv6 em sua VPC ou sub-rede, mas deseja continuar usando sua VPC ou sub-rede para criar e se comunicar com recursos IPv4, é possível desassociar o bloco CIDR IPv6.

Para desassociar um bloco CIDR IPv6, você deve primeiro cancelar a atribuição de quaisquer endereços IPv6 atribuídos a qualquer instância em sua sub-rede. Para obter mais informações, consulte Cancelar a atribuição de um endereço IPv6 de uma instância (p. 124).

Para desassociar um bloco CIDR IPv6 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 Subnets (Sub-redes).
3. Selecione sua sub-rede e escolha Actions (Ações), Edit CIDRs IPv6 (Editar CIDRs IPv6).
4. Remova o bloco CIDR IPv6 da sub-rede escolhendo o ícone de cruz.
5. Escolha Fechar.

Para desassociar um bloco CIDR IPv6 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, selecione Your VPCs (Suas VPCs).
3. Selecione sua VPC, escolha Ações, Edit CIDRs.
4. Remova o bloco CIDR IPv6 escolhendo o ícone de cruz.
5. Escolha Fechar.

> **Note**
>
> A desassociação de um bloco CIDR IPv6 não exclui automaticamente quaisquer regras do security group, as regras do Network ACL ou as rotas da tabela de rotas que você configurou para redes IPv6. Você deve modificar manualmente ou excluir essas regras ou rotas.

Como alternativa, você pode usar uma ferramenta de linha de comando.

Para desassociar um bloco CIDR IPv6 de uma sub-rede usando uma ferramenta de linha de comando

- disassociate-subnet-cidr-block (CLI da AWS)
- Unregister-EC2SubnetCidrBlock (AWS Tools for Windows PowerShell)

Para desassociar um bloco CIDR IPv6 de uma VPC usando uma ferramenta de linha de comando

- disassociate-vpc-cidr-block (CLI da AWS)
- Unregister-EC2VpcCidrBlock (AWS Tools for Windows PowerShell)

Excluir sua VPC

Para excluir uma VPC usando o console da VPC, primeiro é necessário encerrar ou excluir os seguintes componentes:

- Todas as instâncias na VPC: para obter informações sobre como encerrar uma instância, consulte Encerrar a instância no Guia do usuário do Amazon EC2 para instâncias do Linux.
- Conexões de emparelhamento de VPC
- Endpoints de interface
- Gateways NAT

Quando uma VPC é excluída usando-se o console da VPC, também excluímos os seguintes componentes da VPC para você:

- Sub-redes
- Grupos de segurança
- Network ACLs
- Tabelas de rotas
- Endpoints de gateway
- Gateways da Internet
- Gateways da Internet apenas de saída
- Opções do DHCP

Se você tiver uma conexão AWS Site-to-Site VPN, não será necessário excluí-la ou os outros componentes relacionados à VPN (como o gateway do cliente e o gateway privado virtual). 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.

Para excluir a VPC usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Encerre todas as instâncias na VPC. Para obter mais informações, consulte Encerrar a instância no Guia do usuário do Amazon EC2 para instâncias do Linux.
3. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
4. No painel de navegação, selecione Your VPCs (Suas VPCs).
5. Selecione a VPC para excluir e escolha Ações, Excluir VPC.
6. Se você tiver uma conexão Site-to-Site VPN, selecione a opção para excluí-la. Caso contrário, deixe-a desmarcada. Escolha Delete VPC (Excluir VPC).

Como alternativa, você pode usar uma ferramenta de linha de comando. Quando uma VPC é excluída usando-se a linha de comando, primeiro é necessário encerrar todas as instâncias e excluir ou desanexar todos os recursos associados, incluindo sub-redes, grupos de segurança personalizados, ACLs de rede personalizadas, tabelas de rotas personalizadas, conexões de emparelhamento de VPC, endpoints, o gateway NAT, o gateway da Internet e o gateway de Internet somente de saída.

Como excluir uma VPC usando uma ferramenta de linha de comando

- delete-vpc (CLI da AWS)
- Remove-EC2Vpc (AWS Tools for Windows PowerShell)

Endereçamento IP na sua VPC

Os endereços IP habilitam recursos na sua VPC para se comunicar com outros e com recursos na Internet. O Amazon EC2 e a Amazon VPC são compatíveis com protocolos de endereçamento IPv4 e IPv6.

Por padrão, o Amazon EC2 e a Amazon VPC usam o protocolo de endereçamento IPv4. Ao criar uma VPC, você deve atribui-la a um bloco CIDR IPv4 (diversos endereços IPv4 privados). Os endereços IPv4 privados não podem ser acessados pela Internet. Para conectar sua instância na Internet ou habilitar a comunicação entres suas instâncias e outros serviços da AWS que têm endpoints públicos, é possível atribuir endereços IPv4 públicos globalmente exclusivos da sua instância.

Como opção, você pode associar um bloco CIDR IPv6 a sua VPC e sub-redes e atribuir endereços IPv6 desse bloco a recursos em sua VPC. Os endereços IPv6 são públicos e podem ser acessados pela Internet.

> **Note**
>
> Para garantir que as instâncias possam se comunicar com a Internet, também é necessário anexar um gateway da Internet à VPC. Para obter mais informações, consulte Gateways da Internet (p. 212).

A VPC pode operar em modo de pilha dupla: seus recursos podem se comunicar por IPv4, IPv6 ou ambos. Os endereços IPv4 e IPv6 são independentes um do outro. Você pode configurar o roteamento e a segurança na sua VPC separadamente para IPv4 e IPv6.

A tabela a seguir resume as diferenças entre IPv4 e IPv6 no Amazon EC2 e na Amazon VPC.

Características e restrições de IPv4 e IPv6

IPv4	IPv6
O formato é de 32 bits, 4 grupos de até 3 dígitos decimais.	O formato é 128 bits, 8 grupos de 4 dígitos hexadecimais.
Padrão e obrigatório para todas as VPCs; não pode ser removido.	Somente assinatura.
O tamanho do bloco CIDR da VPC pode ser de /16 a /28.	O tamanho do bloco CIDR da VPC é fixo em /56.
O tamanho do bloco CIDR da sub-rede pode ser de /16 a /28.	O tamanho do bloco CIDR da sub-rede é fixo em /64.
Você pode escolher o bloco CIDR IPv4 privado para a sua VPC.	Escolhemos o bloco CIDR IPv6 para a sua VPC a partir do grupo da Amazon de endereços IPv6. Você não pode selecionar seu próprio intervalo.
Existe uma diferença entre endereços IP públicos e privados. Para permitir a comunicação com a Internet, um endereço IPv4 público é mapeado para um endereço IPv4 primário privado pela tradução de endereço de rede (NAT).	Não existem diferenças entre endereços IP públicos e privados. Os endereços IPv6 são públicos.
Compatível com todos os tipos de instâncias.	Compatível com todos os tipos de instância da geração atual e com os tipos de instância C3, R3 e I2 das gerações anteriores. Para obter mais informações, consulte Tipos de instância.
Compatível com conexões EC2-Classic e EC2-Classic com uma VPC pelo ClassicLink.	Não é compatível com conexões EC2-Classic e EC2-Classic com uma VPC pelo ClassicLink.
Compatível com todos as AMIs.	Compatível automaticamente com AMIs que são configuradas para DHCPv6. As versões do Amazon Linux 2016.09.0 e posteriores e do Windows Server 2008 R2 e posteriores são configuradas para DHCPv6. Para outras

IPv4	IPv6
	AMIs, você deve configurar manualmente sua instância (p. 132) para reconhecer quaisquer endereços IPv6 atribuídos.
Uma instância recebe um nome de host DNS privado fornecido pela Amazon que corresponde ao seu endereço IPv4 privado e, se aplicável, um nome de host DNS público que corresponde ao IPv4 público ou endereço IP elástico.	Os nomes de host DNS fornecidos pela Amazon não são compatíveis.
Os endereços IPv4 elásticos são compatíveis.	Os endereços IPv6 elásticos não são compatíveis.
Com suporte para gateways do cliente, gateways privados virtuais, dispositivos NAT e VPC endpoints.	Não há suporte para gateways do cliente, gateways privados virtuais, dispositivos NAT e VPC endpoints.

Oferecemos suporte ao tráfego IPv6 por um gateway privado virtual para uma conexão do AWS Direct Connect. Para obter mais informações, consulte o Guia do usuário do AWS Direct Connect.

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. Quando você inicia uma instância em uma VPC, um endereço IP privado primário do intervalo de endereços IPv4 da sub-rede é atribuído à interface de rede (eth0) padrão da instância. Cada instância também recebe um nome de host DNS privado (interno) que resolve o endereço IP privado da instância. 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 para instâncias do Linux.

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 encerrada. Para obter mais informações sobre endereços IP primários e secundários, consulte Vários endereços IP no Guia do usuário do Amazon EC2 para instâncias do Linux.

> **Note**
>
> 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 o AWS Direct Connect.

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). Portanto, quando você inicia uma instância em uma sub-rede que possui esse atributo habilitado, um

endereço IP público é atribuído à interface de rede primária (eth0) criada para a instância. Um endereço IP público é mapeado para o endereço IP privado primário pela tradução de endereço de rede (NAT).

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

- Modificando o atributo de endereçamento IP público de sua sub-rede. Para obter mais informações, consulte Modificar o atributo de endereçamento IPv4 público para a sub-rede (p. 122).
- 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. Para obter mais informações, consulte Atribuir um endereço IPv4 público durante a execução da instância (p. 122).

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. Você não pode associar manualmente ou desassociar um endereço IP público. Em vez disso, em certos casos, liberamos o endereço IP público de sua instância ou atribuímos um novo. Para obter mais informações, consulte Endereços IP públicos no Guia do usuário do Amazon EC2 para instâncias do Linux.

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 Endereços IP elásticos (p. 277).

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 obter mais informações, consulte Usar DNS com a VPC (p. 262).

Endereços IPv6

Você pode opcionalmente associar um bloco CIDR IPv6 a sua VPC e sub-redes. Para obter mais informações, consulte os tópicos a seguir:

- Associar um bloco CIDR IPv6 à sua VPC (p. 113)
- Associar um bloco CIDR IPv6 à sub-rede (p. 114)

A sua instância em uma VPC recebe um endereço IPv6 se um bloco CIDR IPv6 estiver associado a sua VPC e sua sub-rede, e se uma das seguintes afirmações for verdadeira:

- Sua sub-rede está configurada para atribuir automaticamente um endereço IPv6 à interface de rede principal de uma instância durante a inicialização.
- Você atribui manualmente um endereço IPv6 à sua instância durante a inicialização.
- Você atribui um endereço IPv6 à sua instância após a inicialização.
- Você atribui um endereço IPv6 a uma interface de rede na mesma sub-rede e anexa a interface de rede a sua instância após a inicialização.

Quando sua instância recebe um endereço IPv6 durante a inicialização, o endereço está associado a interface de rede primária (eth0) de instância. Você pode desassociar o endereço IPv6 da interface de rede primária. Não oferecemos suporte a nomes de host DNS IPv6 da sua instância.

Um endereço IPv6 persiste quando você para e inicia a instância, e é liberado quando você encerra a instância. Não é possível atribuir novamente um endereço IPv6 enquanto ele estiver atribuído a outra interface de rede. Primeiro é necessário cancelar a atribuição.

Você pode atribuir endereços IPv6 adicionais à instância atribuindo-os a uma interface de rede anexada à instância. O número de endereços IPv6 que você pode atribuir a uma interface de rede e o número de interfaces de rede que você pode anexar a uma instância varia de acordo com o tipo de instância. Para obter mais informações, consulte Endereços IP por interface de rede por tipo de instância no Guia do usuário do Amazon EC2.

Os endereços IPv6 são globalmente exclusivos e, portanto, acessíveis pela Internet. Você pode controlar se as instâncias são acessíveis através de seus endereços IPv6, controlando o roteamento da sua sub-rede ou usando o security group e as regras de Network ACL. Para obter mais informações, consulte Privacidade do tráfego entre redes na Amazon VPC (p. 158).

Para obter mais informações sobre intervalos de endereço IPv6 reservados, consulte Registro de endereço para finalidades especiais IANA IPv6 e RFC4291.

Comportamento do endereçamento IP para a sub-rede

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 (eth0) criada para uma instância quando você inicia uma instância nesta sub-rede.

Independentemente do atributo da sub-rede, você ainda pode substituir esta configuração para uma instância específica durante a inicialização. Para obter mais informações, consulte Atribuir um endereço IPv4 público durante a execução da instância (p. 122) e Atribuir um endereço IPv6 durante a execução de instância (p. 123).

Usar 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 trazer 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 Bring your own IP addresses (BYOIP) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Trabalhar com endereços IP

Você pode modificar o comportamento de endereçamento IP da sua sub-rede, atribuir um endereço IPv4 público à sua instância durante a inicialização e atribuir ou cancelar a atribuição dos endereços IPv6 para e a partir da sua instância.

Tarefas

Modificar o atributo de endereçamento IPv4 público para a 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.

Para modificar o comportamento de endereçamento IPv4 público da sua 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 Ações de sub-redes, Modificar configurações de IP de atribuição automática.
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.

Modificar o atributo de endereçamento IPv6 para a sub-rede

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 IPv6 público da sua 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 Ações de sub-redes, Modificar configurações de IP de atribuição automática.
4. 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.

Atribuir um endereço IPv4 público durante a execução da instância

Você pode controlar se sua instância em uma sub-rede padrão ou não padrão é atribuída a um endereço IPv4 público durante a inicialização.

> **Important**
>
> Você não pode desassociar manualmente o endereço público IPv4 da sua instância após a inicialização. Em vez disso, ele é automaticamente iniciado em certos casos, após o qual

você não pode reutilizá-lo. Se você precisar de um endereço IP público persistente que é possível associar ou desassociar à vontade, associe um endereço IP elástico à instância após a inicialização em vez disso. Para obter mais informações, consulte Endereços IP elásticos (p. 277).

Para atribuir um endereço IPv4 público a uma instância durante a inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Launch Instance (Executar instância).
3. Selecione uma AMI e um tipo de instância e escolha Next: Configure Instance Details.
4. Na página Configure Instance Details, em Network, selecione uma VPC. A lista Auto-assign Public IP é exibida. Escolha Enable ou Disable para substituir a configuração padrão da sub-rede.
5. Siga as etapas nas páginas a seguir do assistente para concluir a configuração da instância. Na página final Review Instance Launch, reveja suas configurações, e escolha Launch para escolher um par de chaves e executar a instância.
6. Na página Instances, selecione a nova instância e visualize o endereço IP público correspondente no campo IPv4 Public IP no painel de detalhes.

   Note

   O endereço de público IPv4 é exibido como uma propriedade de interface de rede no console, mas mapeou o endereço IPv4 privado primário pelo NAT. Portanto, se você inspecionar as propriedades de interface de rede em sua instância, por exemplo, através de `ipconfig` em uma instância do Windows ou `ifconfig` em uma instância do Linux, o endereço IP público não será exibido. Para determinar o endereço IP público da sua instância dentro da instância, você pode usar os metadados de instância. Para obter mais informações, consulte Metadados de instância e dados do usuário.

Este recurso só está disponível durante a inicialização. No entanto, se você atribuir ou não um endereço IPv4 público à sua instância durante a inicialização, você pode associar um endereço IP elástico a sua instância depois que ele for iniciado. Para obter mais informações, consulte Endereços IP elásticos (p. 277).

Atribuir um endereço IPv6 durante a execução de instância

Você pode atribuir automaticamente um endereço IPv6 para sua instância durante a inicialização. Para fazer isso, você deve iniciar sua instância em uma VPC e uma sub-rede que tenha um bloco CIDR IPv6 associado (p. 113). O endereço IPv6 é atribuído do intervalo da sub-rede e é atribuído à interface de rede principal (eth0).

Para atribuir automaticamente um endereço IPv6 a uma instância durante a execução

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Selecione Launch Instance (Executar instância).
3. Selecione um AMI e um tipo de instância e selecione Next: Configure Instance Details (Próximo: configurar detalhes da instância).

   Note

   Selecione um tipo de instância que ofereça suporte a endereços IPv6.
4. Na página Configure Instance Details, selecione uma VPC em Rede e uma sub-rede em Sub-rede. Em Auto-assign IPv6 IP, escolha Habilitar.
5. Siga as etapas restantes no assistente para iniciar a instância.

Alternativamente, se você quiser atribuir um endereço IPv6 específico do intervalo de sub-rede à sua instância durante a inicialização, você pode atribuir o endereço à interface de rede primária da sua instância.

Para atribuir um endereço IPv6 específico a uma instância durante a inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Selecione Launch Instance (Executar instância).
3. Selecione um AMI e um tipo de instância e selecione Next: Configure Instance Details (Próximo: configurar detalhes da instância).

   Note

   Selecione um tipo de instância que ofereça suporte a endereços IPv6.
4. Na página Configure Instance Details, selecione uma VPC em Rede e uma sub-rede em Sub-rede.
5. Acesse a seção Interfaces de rede. Para a interface de rede eth0, em IPs IPv6, selecione Adicionar IP.
6. Digite um endereço IPv6 do intervalo da sub-rede.
7. Siga as etapas restantes no assistente para iniciar a instância.

Para obter mais informações sobre como atribuir vários endereços IPv6 à sua instância durante a inicialização, consulte Trabalhar com vários endereços IPv6 no Guia do usuário do Amazon EC2 para instâncias do Linux

Atribuir um endereço IPv6 a uma instância

Se a sua instância estiver em uma VPC e uma sub-rede com um bloco CIDR IPv6 associado (p. 113), você poderá usar o console do Amazon EC2 para atribuir um endereço IPv6 à sua instância a partir do intervalo da sub-rede.

Para associar um endereço IPv6 à sua instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias e selecione sua instância.
3. Escolha Actions (Ações), Networking (Redes), Manage IP Addresses (Gerenciar endereços IP).
4. Em Endereços IPv6, escolha Atribuir novo IP. Você pode especificar um endereço IPv6 no intervalo da sub-rede ou deixar o valor Auto-assign para permitir que a Amazon escolha um endereço IPv6 para você.
5. Escolha Salvar.

Como alternativa, você pode atribuir um endereço IPv6 a sua interface de rede. Para obter mais informações, consulte Atribuir um endereço IPv6 no tópico Interfaces de rede elástica no Guia do usuário do Amazon EC2 para instâncias do Linux

Cancelar a atribuição de um endereço IPv6 de uma instância

Se você não precisar mais de um endereço IPv6 para sua instância, poderá desassociá-lo da instância usando o console do Amazon EC2.

Para desassociar um endereço IPv6 da sua instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias e selecione sua instância.

3. Escolha Actions (Ações), Networking (Redes), Manage IP Addresses (Gerenciar endereços IP).
4. Em Endereços IPv6, selecione Cancelar atribuição para os de endereços IPv6.
5. Escolha Salvar.

Alternativamente, você pode desassociar um endereço IPv6 a partir de uma interface de rede. Para obter mais informações, consulte Desassociar um endereço IPv6 no tópico Interfaces de rede elástica no Guia do usuário do Amazon EC2 para instâncias do Linux.

Visão geral da API e dos comandos

Você pode executar as tarefas descritas nesta página usando a linha de comando ou uma API. Para obter mais informações sobre as interfaces de linha de comando e uma lista das APIs disponíveis, consulte Acessar a Amazon VPC (p. 1).

Atribuir um endereço público IPv4 durante a inicialização

- Use a opção `--associate-public-ip-address` ou `--no-associate-public-ip-address` com o comando run-instances. (CLI da AWS)
- Use o parâmetro `-AssociatePublicIp` com o comando New-EC2Instance. (AWS Tools for Windows PowerShell)

Atribuir um endereço IPv6 durante a inicialização

- Use a opção `--ipv6-addresses` com o comando run-instances (CLI da AWS)
- Use o parâmetro `-Ipv6Addresses` com o comando New-EC2Instance (AWS Tools for Windows PowerShell)

Modificar o comportamento de endereçamento IP de uma sub-rede

- modify-subnet-attribute (CLI da AWS)
- Edit-EC2SubnetAttribute (AWS Tools for Windows PowerShell)

Atribuir um endereço IPv6 a uma interface de rede

- assign-ipv6-addresses (CLI da AWS)
- Register-EC2Ipv6AddressList (AWS Tools for Windows PowerShell)

Desassociar um endereço IPv6 de uma interface de rede

- unassign-ipv6-addresses (CLI da AWS)
- Unregister-EC2Ipv6AddressList (AWS Tools for Windows PowerShell)

Migração para o IPv6

Se você possuir uma VPC existente que ofereça suporte somente para IPv4 e recursos na sub-rede que sejam configurados para usar somente o IPv4, você pode habilitar o suporte ao IPv6 para a VPC e recursos. A VPC pode operar em modo de pilha dupla: 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.

Note

Essas informações pressupõem que você tenha uma VPC existente com sub-redes públicas e privadas. Para obter informações sobre como configurar uma VPC para uso com IPv6, consulte the section called “Visão geral de IPv6” (p. 22).

A tabela a seguir fornece uma visão geral das etapas para habilitar sua VPC e sub-redes para usarem o IPv6.

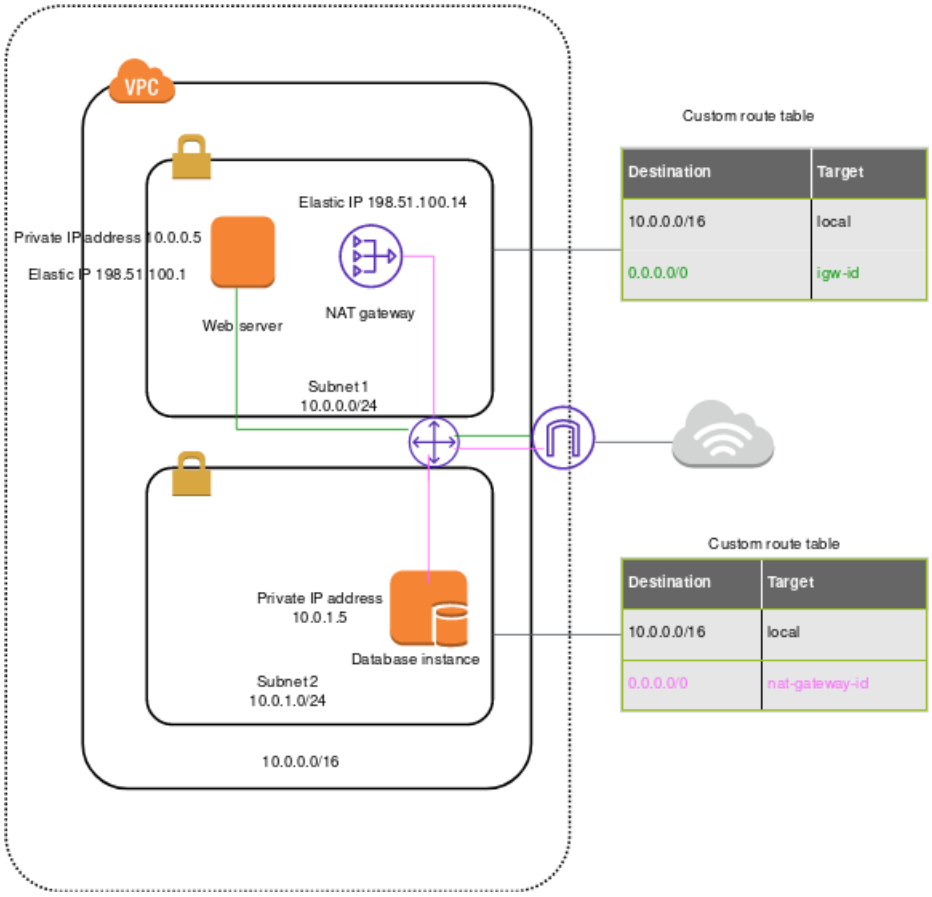
Etapa	Observações
Etapa 1: Associar um bloco CIDR IPv6 com a VPC e as sub-redes (p. 129)	Associe um bloco CIDR IPv6 fornecido pela Amazon com a VPC e com as sub-redes.
Etapa 2: Atualizar as tabelas de rotas (p. 130)	Atualize as tabelas de rota para encaminhar o tráfego IPv6. Para uma sub-rede pública, 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 (p. 130)	Atualize as regras do security group 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 network ACL para controlar o fluxo de tráfego para e a partir da sub-rede, você deve incluir regras para o tráfego IPv6.
Etapa 4: Alterar o tipo de instância (p. 131)	Se o tipo de instância não oferecer suporte a IPv6, altere o tipo de instância.
Etapa 5: Atribuir endereços IPv6 às instâncias (p. 132)	Atribua endereços IPv6 às instâncias a partir do intervalo de endereços IPv6 da sub-rede.
Etapa 6: (Opcional) Configurar o IPv6 nas instâncias (p. 132)	Se a instância for iniciada a partir de uma AMI que não esteja configurada para usar DHCPv6, você deve configurar a instância manualmente para que reconheça um endereço IPv6 atribuído a ela.

Antes de migrar para o IPv6, certifique-se de ter lido os recursos do endereçamento IPv6 para a Amazon VPC: Características e restrições de IPv4 e IPv6 (p. 118).

Tópicos

Exemplo: Habilitar o IPv6 em uma VPC com sub-rede pública e privada

Neste exemplo, a VPC possui uma sub-rede pública e privada. Você tem uma instância de banco de dados na sub-rede privada que possui comunicação de saída com a Internet por meio de um gateway NAT na VPC. Você tem um servidor web voltado para o público na sub-rede pública que possui acesso à Internet por meio do gateway de Internet. O diagrama a seguir ilustra a arquitetura da VPC.



O security group para o servidor da web (`sg-11aa22bb11aa22bb1`) tem as seguintes regras de entrada:

Tipo	Protocolo	Intervalo de portas	Origem	Comentário
Todo o tráfego	Tudo	Todos	sg-33cc44dd33cc44dd3	Concede acesso de entrada para todo o tráfego de instâncias associadas ao sg-33cc44dd33cc44dd3 (a instância do banco de dados).
HTTP	TCP	80	0.0.0.0/0	Permite tráfego de entrada da Internet via HTTP.

Tipo	Protocolo	Intervalo de portas	Origem	Comentário
HTTPS	TCP	443	0.0.0.0/0	Permite tráfego de entrada da Internet via HTTPS.
SSH	TCP	22	203.0.113.123/32	Permite o acesso SSH de entrada a partir do seu computador local. Por exemplo, quando você precisa se conectar à instância para executar tarefas de administração.

O security group para a instância do banco de dados (`sg-33cc44dd33cc44dd3`) tem a seguinte regra de entrada:

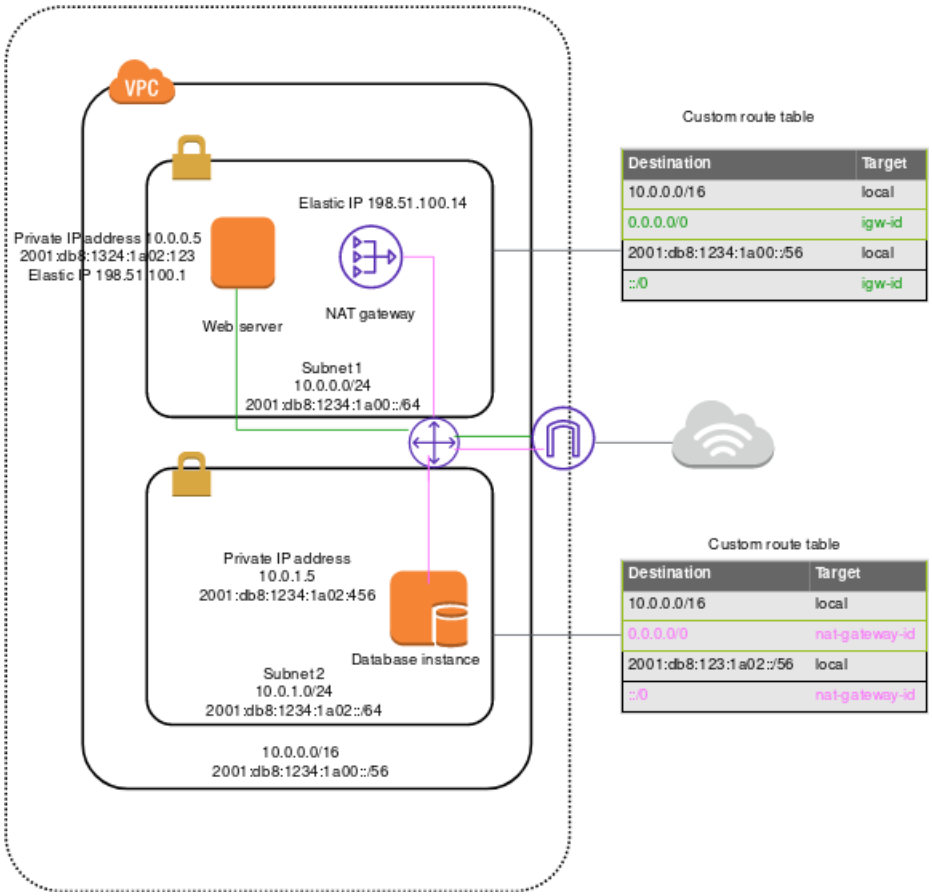
Tipo	Protocolo	Intervalo de portas	Origem	Comentário
MySQL	TCP	3306	sg-11aa22bb11aa22bb1	Concede acesso de entrada para o tráfego de MySQL de instâncias associadas ao sg-11aa22bb11aa22bb1 (a instância do servidor web).

Ambos os security groups têm a regra de saída padrão que permite todo o tráfego IPv4 de saída e nenhuma outra regra de saída.

O servidor da web é do tipo de instância `t2.medium`. O servidor de banco de dados é um `m3.large`.

Você deseja que a VPC e os recursos estejam habilitados para IPv6 e também que eles operem no modo pilha dupla. Em outras palavras, você quer usar o endereçamento IPv6 e IPv4 entre recursos da VPC e recursos via Internet.

Depois de concluídas as etapas, a VPC terá a seguinte configuração:



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, selecione Your VPCs (Suas VPCs).
3. Selecione sua VPC, escolha Ações, Edit CIDRs.
4. Escolha Add IPv6 CIDR (Adicionar CIDR IPv6), selecione uma das seguintes opções e escolha Select CIDR (Selecionar CIDR):

   - Amazon-provided IPv6 CIDR block (Bloco CIDR IPv6 fornecido pela Amazon): solicita 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.
   - IPv6 CIDR owned by me (CIDR IPv6 pertencente a mim): (BYOIP) aloca um bloco CIDR IPv6 do seu grupo de endereços IPv6. Para Pool (Grupo), escolha o grupo de endereços IPv6 a partir do qual alocar o bloco CIDR IPv6.

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 sua sub-rede e escolha Ações de sub-redes, Edit CIDRs IPv6.
4. Escolha Adicionar CIDR IPv6. Especifique o par hexadecimal para a sub-rede (por exemplo, `00`) e confirme a entrada escolhendo o ícone de seleção.
5. Escolha Fechar. Repita as etapas para as outras sub-redes da VPC.

Para obter mais informações, consulte Dimensionamento da VPC e da sub-rede para IPv6 (p. 108).

Etapa 2: Atualizar as tabelas de rotas

Para uma sub-rede pública, você deverá atualizar a tabela de rotas para permitir que instâncias (como servidores web) usem o gateway de Internet para tráfego IPv6.

Para uma sub-rede privada, você deve atualizar a tabela de rotas para permitir que instâncias (como instâncias do banco de dados) usem um gateway de Internet de somente saída para tráfego IPv6.

Para atualizar sua tabela de rotas para um sub-rede pública

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Tabela de rotas e selecione a tabela de rotas associada à sub-rede pública.
3. Na guia Routes, escolha Edit.
4. Escolha Add another route. Especifique `::/0` para Destination (Destino), selecione o ID do gateway de Internet para Target (Alvo) e selecione Save (Salvar).

Para atualizar sua tabela de rotas para uma sub-rede privada

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. Se você estiver usando um dispositivo NAT na sua sub-rede privada, ele não oferecerá suporte a tráfego IPv6. Em vez disso, crie um gateway de Internet somente de saída para sua sub-rede privada para permitir comunicação de saída para a Internet via IPv6 e evitar comunicação de entrada. Um gateway de Internet somente de saída oferece suporte somente ao tráfego IPv6. Para obter mais informações, consulte Gateways da Internet apenas de saída (p. 218).
3. No painel de navegação, escolha Route Tables e selecione a tabela de rotas associada à sub-rede privada.
4. Na guia Routes, escolha Edit.
5. Escolha Add another route. Para Destination, especifique `::/0`. Para Target (Destino), selecione o ID do gateway da Internet somente de saída e depois selecione Save (Salvar).

Para obter mais informações, consulte Exemplo de opções de roteamento (p. 291).

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 security group para incluir regras para endereços IPv6.

Por exemplo, no exemplo acima, atualize o security group 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 para o security group do banco de dados. A regra que permite toda a comunicação de `sg-11aa22bb11aa22bb1` inclui a comunicação IPv6 por padrão.

Para atualizar as regras do security group

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

2. No painel de navegação, escolha Security Groups e selecione o security group do servidor da web.
3. Na guia Inbound Rules, escolha Edit.
4. Para cada regra, escolha Add another rule, e escolha Save quando tiver concluído. Por exemplo, para adicionar uma regra que permite todo o tráfego HTTP pelo IPv6, para Type, selecione HTTP e para Source insira `::/0`.

Por padrão, uma regra de saída que permite o tráfego IPv6 seja adicionado automaticamente aos security groups quando você associar um bloco CIDR IPv6 à VPC. No entanto, se você modificou as regras de saída originais para o security group, esta regra não será adicionada automaticamente e você deverá adicionar regras de saída equivalentes para o tráfego IPv6. Para obter mais informações, consulte Grupos de segurança para a VPC (p. 180).

Atualizar as regras de network ACL

Se você associar um bloco CIDR IPv6 à VPC, automaticamente adicionaremos regras à network ACL padrão para permitir o tráfego IPv6, desde que as regras padrão não tenham sido modificadas. Se você modificou a network ACL padrão ou se você criou uma network ACL personalizada com regras para controlar o fluxo de tráfego para e a partir da sub-rede, você deve adicionar manualmente regras para o tráfego IPv6. Para obter mais informações, consulte Network ACLs (p. 190).

Etapa 4: Alterar o tipo de instância

Todos os tipos de instância da geração atual oferecem suporte a IPv6. Para obter mais informações, consulte Tipos de instância.

Se o tipo de instância não oferece suporte a IPv6, redimensione a instância para um tipo de instância suportado. No exemplo acima, a instância do banco de dados é do tipo `m3.large` que não oferece suporte ao IPv6. Você deve redimensionar a instância para um tipo de instância compatível, como por exemplo, `m4.large`.

Para redimensionar a instância, esteja ciente das limitações de compatibilidade. Para obter mais informações, consulte Compatibilidade para redimensionamento de instâncias no Guia do usuário do Amazon EC2 para instâncias do Linux. Nesse cenário, se a instância de banco de dados foi iniciada a partir de um AMI que usa a virtualização HVM, você pode redimensioná-la para um tipo de instância `m4.large` usando o procedimento a seguir.

> **Important**
>
> Para redimensionar a instância, você deve interrompê-la. Parar e iniciar uma instância causa a alteração do endereço público IPv4 para a instância, se houver um. Se você possuir dados armazenados em volumes de armazenamento de instância, os dados serão apagados.

Para redimensionar a instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instâncias e selecione a instância do banco de dados.
3. Escolha Ações, Instance State, Parar.
4. Na caixa de diálogo para confirmação, escolha Yes, parar.
5. Com a instância ainda selecionada, escolha Ações, Instance Settings, Change Instance Type.
6. Para Tipo de instância, escolha o novo tipo de instância e, em seguida, selecione Aplicar.
7. Para reiniciar a instância interrompida, selecione a instância e escolha Ações, Instance State, Iniciar. Na caixa de diálogo para confirmação, escolha Sim, iniciar.

Se a instância for uma instance store-backed AMI, você não poderá redimensioná-la usando o procedimento anterior. Em vez disso, você poderá criar uma instance store-backed AMI a partir da

instância e iniciar uma nova instância a partir da AMI usando um novo tipo de instância. Para obter mais informações, consulte Criar uma AMI do Linux com armazenamento de instâncias no Guia do usuário do Amazon EC2 para instâncias do Linux e Criar uma AMI do Windows com armazenamento de instâncias no Guia do usuário do Amazon EC2 para instâncias do Windows.

Você pode não conseguir migrar para um novo tipo de instância se houver limitações de compatibilidade. Por exemplo, se a instância for iniciada a partir de uma AMI que usa a virtualização PV, o único tipo de instância que admitirá a virtualização PV e IPv6 é o C3. Esse tipo de instância pode não ser adequado às suas necessidades. Nesse caso, talvez seja necessário reinstalar o software em uma AMI HVM base e iniciar uma nova instância.

Se você iniciar uma instância de uma nova AMI, você poderá atribuir um endereço IPv6 à instância durante o lançamento.

Etapa 5: Atribuir endereços IPv6 às instâncias

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 à interface de rede primária (eth0) para a instância.

Para atribuir um endereço IPv6 à instância

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 e escolha Ações, Redes, Manage IP Addresses.
4. Em Endereços IPv6, escolha Atribuir novo IP. Você pode inserir um endereço IPv6 específico do intervalo da sub-rede ou pode deixar o valor padrão `Auto-Assign` para permitir que a Amazon escolha um para você.
5. Escolha Yes, Update.

Como alternativa, se você executar uma nova instância (por exemplo, se você não conseguiu alterar o tipo de instância e, em vez disso, criou uma AMI), poderá atribuir um endereço IPv6 durante a execução.

Para atribuir um endereço IPv6 a uma instância durante a execução

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Selecione uma AMI e um tipo de instância compatível com IPv6 e escolha Next: Configure Instance Details.
3. Na página Configure Instance Details, selecione a VPC em Network e uma sub-rede em Sub-rede. Em Auto-assign IPv6 IP, selecione Habilitar.
4. Siga as etapas restantes no assistente para iniciar a instância.

É possível conectar-se a uma instância usando seu endereço IPv6. Se estiver se conectando de um computador local, verifique se ele tem um endereço IPv6 e se está configurado para usar IPv6. Para obter mais informações, consulte Conectar-se à instância do Linux no Guia do usuário do Amazon EC2 para instâncias do Linux e Conectar-se à instância do Windows no Guia do usuário do Amazon EC2 para instâncias do Windows.

Etapa 6: (Opcional) Configurar o IPv6 nas instâncias

Se você executou a instância usando o Amazon Linux 2016.09.0 ou posterior, o Windows Server 2008 R2 ou posterior ou o Ubuntu Server 2018 ou posterior, a instância está configurada para IPv6, e nenhuma etapa adicional é necessária.

Se a instância foi executada a partir de uma AMI diferente, ela talvez não esteja configurada para IPv6 e DHCPv6, o que significa que qualquer endereço IPv6 que você atribuir à instância não será reconhecido automaticamente na interface de rede primária.

Para verificar DHCPv6 no Linux

Use o comando ping6 da seguinte forma.

```
$ ping6 ipv6.google.com
```

Para verificar DHCPv6 no Windows

Use o comando ping da seguinte forma.

```
C:\> ping -6 ipv6.google.com
```

Se a instância ainda não estiver configurada, você poderá configurá-la manualmente, conforme mostrado nos procedimentos a seguir.

Configuração manual, pelo sistema operacional

- Amazon Linux (p. 133)
- Ubuntu (p. 134)
- RHEL/CentOS (p. 136)
- Windows (p. 137)

Amazon Linux

Para configurar sua instância do Amazon Linux

1. Conecte-se à instância usando o endereço IPv4 público da mesma.
2. Obtenha os pacotes de software mais recentes para a instância:

   ```
   sudo yum update -y
   ```
3. Usando um editor de texto de sua escolha, abra `/etc/sysconfig/network-scripts/ifcfg-eth0` e localize a seguinte linha:

   ```
   IPV6INIT=no
   ```

   Substitua a linha encontrada pelo seguinte:

   ```
   IPV6INIT=yes
   ```

   Adicione as duas linhas a seguir e salve as alterações:

   ```
   DHCPV6C=yes
   DHCPV6C_OPTIONS=-nw
   ```
4. Abra `/etc/sysconfig/network`, remova as seguintes linhas e salve as alterações:

   ```
   NETWORKING_IPV6=no
   IPV6INIT=no
   IPV6_ROUTER=no
   IPV6_AUTOCONF=no
   ```

```
IPV6FORWARDING=no
IPV6TO4INIT=no
IPV6_CONTROL_RADVD=no
```

5. Abra `/etc/hosts`, substitua o conteúdo pelo seguinte e salve as alterações:

```
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost6 localhost6.localdomain6
```

6. Reinicie a instância. Reconecte-se à instância e use o comando `ifconfig` para verificar se o endereço IPv6 é reconhecido na interface de rede primária.

Ubuntu

Você pode configurar a instância Ubuntu para reconhecer dinamicamente qualquer endereço IPv6 atribuído à interface de rede. Se a instância não tiver um endereço IPv6, esta configuração pode fazer com que o tempo de inicialização da instância seja prolongado em até 5 minutos.

Tópicos

Ubuntu Server 16

Essas etapas devem ser executadas como usuários raiz.

Para configurar uma instância do Ubuntu Server 16

1. Conecte-se à instância usando o endereço IPv4 público da mesma.
2. Visualize o conteúdo do arquivo `/etc/network/interfaces.d/50-cloud-init.cfg`:

```
cat /etc/network/interfaces.d/50-cloud-init.cfg
```

```
# This file is generated from information provided by
# the datasource.  Changes to it will not persist across an instance.
# To disable cloud-init's network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp
```

   Verifique se o dispositivo de rede de loopback (`lo`) está configurado e anote o nome da interface de rede. Neste exemplo, o nome da interface de rede é `eth0`; o nome pode ser diferente dependendo do tipo de instância.
3. Crie o arquivo `/etc/network/interfaces.d/60-default-with-ipv6.cfg` e adicione a seguinte linha. Se necessário, substitua `eth0` pelo nome da interface de rede obtida na etapa acima.

```
iface eth0 inet6 dhcp
```

4. Reinicie a instância ou reinicie a interface de rede executando o seguinte comando. Se necessário, substitua `eth0` pelo nome da interface de rede.

```
sudo ifdown eth0 ; sudo ifup eth0
```

5. Reconecte-se à instância e use o comando `ifconfig` para verificar se o endereço IPv6 está configurado na interface de rede primária.

Para configurar o IPv6 usando dados do usuário

- Você pode iniciar uma nova instância do Ubuntu e garantir que qualquer endereço IPv6 atribuído à instância seja configurado automaticamente na interface de rede, especificando os seguintes dados do usuário durante o lançamento:

```
#!/bin/bash
echo "iface eth0 inet6 dhcp" >> /etc/network/interfaces.d/60-default-with-ipv6.cfg
dhclient -6
```

  Nesse caso, não é necessário conectar-se à instância para configurar o endereço IPv6.

  Para obter mais informações, consulte Executar comandos na instância do Linux na inicialização no Guia do usuário do Amazon EC2 para instâncias do Linux.

Ubuntu Server 14

Se estiver usando o Ubuntu Server 14, você deve incluir uma solução alternativa para um problema conhecido que ocorre ao reiniciar uma interface de rede de pilha dupla (o reinício resulta em um tempo limite prolongado durante o qual a instância não está acessível).

Essas etapas devem ser executadas como usuários raiz.

Para configurar uma instância do Ubuntu Server 14

1. Conecte-se à instância usando o endereço IPv4 público da mesma.
2. Edite o `/etc/network/interfaces.d/eth0.cfg` arquivo a fim de que ele contenha:

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp
    up dhclient -6 $IFACE
```

3. Reinicie a instância:

```
sudo reboot
```

4. Reconecte-se à instância e use o comando `ifconfig` para verificar se o endereço IPv6 está configurado na interface de rede primária.

Iniciar o cliente DHCPv6

Como alternativa, para abrir o endereço IPv6 para a interface de rede imediatamente sem qualquer configuração adicional, você pode iniciar o cliente DHCPv6 na instância. No entanto, o endereço IPv6 não será mantido na interface de rede após a reinicialização.

Para iniciar o cliente DHCPv6 no Ubuntu

1. Conecte-se à instância usando o endereço IPv4 público da mesma.

2. Inicie o cliente DHCPv6:

```
sudo dhclient -6
```

3. Use o comando `ifconfig` para verificar se o endereço IPv6 é reconhecido na interface de rede primária.

RHEL/CentOS

O RHEL 7.4 e o CentOS 7 e posteriores usam cloud-init para configurar a interface de rede e gerar o arquivo `/etc/sysconfig/network-scripts/ifcfg-eth0`. Você pode criar um arquivo de configuração `cloud-init` personalizado para ativar o DHCPv6, que gera um arquivo `ifcfg-eth0` com configurações que ativam o DHCPv6 após cada reinicialização.

> **Note**
>
> Devido a um problema conhecido, se você estiver usando RHEL/CentOS 7.4 com a versão mais recente de cloud-init-0.7.9, essas etapas podem resultar na perda de conectividade com a instância após a reinicialização. Como alternativa, edite manualmente o arquivo `/etc/sysconfig/network-scripts/ifcfg-eth0`.

Para configurar uma instância RHEL/CentOS usando cloud-init

1. Conecte-se à instância usando o endereço IPv4 público da mesma.
2. Usando um editor de texto de sua escolha, crie um arquivo personalizado, como:

```
/etc/cloud/cloud.cfg.d/99-custom-networking.cfg
```

3. Adicione as linhas a seguir ao seu arquivo e salve as alterações:

```
network:
  version: 1
  config:
  - type: physical
    name: eth0
    subnets:
      - type: dhcp
      - type: dhcp6
```

4. Usando um editor de texto de sua escolha, adicione a seguinte linha ao arquivo específico da interface em `/etc/sysctl.d`. Se você desabilitou a Nomenclatura consistente de dispositivos de rede, o nome da interface de rede é `ethX`, ou a interface secundária.

```
net.ipv6.conf.network-interface-name.accept_ra=1
```

   No exemplo a seguir, a interface de rede é `en5`.

```
net.ipv6.conf.en5.accept_ra=1
```

5. Reinicie a instância.
6. Reconecte-se à instância e use o comando ifconfig para verificar se o endereço IPv6 está configurado na interface de rede primária.

Como alternativa, você pode usar o procedimento a seguir para modificar o arquivo `/etc/sysconfig/network-scripts/ifcfg-eth0` diretamente. Você deve usar esse método com as versões anteriores do RHEL e CentOS que não são compatíveis com o cloud-init.

Para configurar uma instância RHEL/CentOS

1. Conecte-se à instância usando o endereço IPv4 público da mesma.
2. Usando um editor de texto de sua escolha, abra `/etc/sysconfig/network-scripts/ifcfg-eth0` e localize a seguinte linha:

   ```
   IPV6INIT="no"
   ```

   Substitua a linha encontrada pelo seguinte:

   ```
   IPV6INIT="yes"
   ```

   Adicione as duas linhas a seguir e salve as alterações:

   ```
   DHCPV6C=yes
   NM_CONTROLLED=no
   ```
3. Abra `/etc/sysconfig/network`, adicione ou modifique a seguinte linha como se segue e salve as alterações:

   ```
   NETWORKING_IPV6=yes
   ```
4. Reinicie a rede na instância executando o comando a seguir:

   ```
   sudo service network restart
   ```

   Você pode usar o comando ifconfig para verificar se o endereço IPv6 é reconhecido na interface de rede primária.

Para solucionar problemas do RHEL 6 ou CentOS 6

Se você reiniciar a rede e for exibida uma mensagem de erro informando que um endereço IPv6 não pode ser obtido, abra `/etc/sysconfig/network-scripts/ifup-eth` e localize a seguinte linha (por padrão, é a linha 327):

```
if /sbin/dhclient "$DHCLIENTARGS"; then
```

Remova as aspas em torno de `$DHCLIENTARGS` e salve as alterações. Reinicie a rede na instância:

```
sudo service network restart
```

Windows

Use os seguintes procedimentos para configurar o IPv6 no Windows Server 2003 e no Windows Server 2008 SP2.

Para garantir que o IPv6 tenha a preferência sobre o IPv4, faça o download da correção chamada Prefira o IPv6 sobre o IPv4 em políticas de prefixo da seguinte página de suporte da Microsoft: https://support.microsoft.com/en-us/help/929852/how-to-disable-ipv6-or-its-components-in-windows.

Para habilitar e configurar o IPv6 no Windows Server 2003

1. Obtenha o endereço IPv6 da instância usando o comando describe-instances da CLI da AWS ou verificando o campo IPv6 IPs para a instância no console do Amazon EC2.
2. Conecte-se à instância usando o endereço IPv4 público da mesma.

3. Dentro da instância, escolha Iniciar, Control Panel, Network Connections, Local Area Connection.
4. Escolha Properties e, em seguida, escolha Instalar.
5. Escolha Protocolo e, em seguida, escolha Adicionar. Em Network Protocol escolha Microsoft TCP/IP version 6e, em seguida, escolha OK.
6. Abra o prompt de comando e abra o shell da rede.

```
netsh
```

7. Mude para o contexto da interface IPv6.

```
interface ipv6
```

8. Adicione o endereço IPv6 à conexão da área local usando o seguinte comando. Substitua o valor do endereço IPv6 pelo endereço IPv6 da instância.

```
add address "Local Area Connection" "ipv6-address"
```

Por exemplo:

```
add address "Local Area Connection" "2001:db8:1234:1a00:1a01:2b:12:d08b"
```

9. Saia do shell de rede.

```
exit
```

10. Use o comando `ipconfig` para verificar se o endereço IPv6 é reconhecido na conexão de área local.

Para habilitar e configurar o IPv6 no Windows Server 2008 SP2

1. Obtenha o endereço IPv6 da instância usando o comando describe-instances da CLI da AWS ou verificando o campo IPv6 IPs para a instância no console do Amazon EC2.
2. Conecte-se à instância do Windows usando o endereço IPv4 público da mesma.
3. Escolha Iniciar, Control Panel.
4. Abra o Network and Sharing Center e, em seguida, abra Network Connections.
5. Clique com o botão direito do mouse em Local Area Network (para a interface de rede) e escolha Properties.
6. Escolha a caixa de seleção Internet Protocol Version 6 (TCP/IPv6) e escolha OK.
7. Abra novamente a caixa de diálogo de propriedades na rede de área local. Escolha Internet Protocol Version 6 (TCP/IPv6) e escolha Properties.
8. Escolha Use the following IPv6 address e faça o seguinte:
   - Em IPv6 Address, insira o endereço IPv6 que você obteve na etapa 1.
   - Em Subnet prefix length, insira `64`.
9. Escolha OK e feche a caixa de diálogo de propriedades.
10. Abra o prompt de comando. Use o comando `ipconfig` para verificar se o endereço IPv6 é reconhecido na conexão de área local.

Trabalhar com VPCs compartilhadas

O compartilhamento de VPC permite que várias contas da AWS criem os recursos de aplicações, como instâncias do Amazon EC2, bancos de dados do Amazon Relational Database Service (RDS), clusters do

Amazon Redshift e funções do AWS Lambda, em Amazon Virtual Private Clouds (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 do 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.

Também é possível compartilhar as Amazon VPCs para aproveitar o roteamento implícito em uma VPC para aplicativos que exigem um alto grau de interconectividade e que estão 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 Amazon VPCs compartilhadas por meio de recursos de conectividade, como AWS PrivateLink, AWS Transit Gateway e emparelhamento de Amazon VPCs. Para obter mais informações sobre os benefícios de compartilhamento de VPCs, consulte Compartilhamento de VPCs: uma nova abordagem ao gerenciamento de várias contas e VPCs.

Tópicos

Pré-requisitos para VPCs compartilhadas

É necessário habilitar o compartilhamento de recursos a partir da conta mestra da sua organização. Para obter informações sobre como habilitar o compartilhamento de recursos, consulte Habilitar o compartilhamento com o AWS Organizations no Guia do usuário do AWS RAM.

Compartilhar uma sub-rede

Você pode compartilhar sub-redes não padrão com outras contas na sua organização. Para fazer isso, crie primeiro um compartilhamento de recurso para as sub-redes e as contas da AWS e unidades organizacionais (ou toda a organização) com quem você deseja compartilhá-las. Para obter informações sobre como criar um compartilhamento de recursos, consulte Criar um compartilhamento de recursos no Guia do usuário do AWS RAM.

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).

Como compartilhar uma sub-rede usando a CLI da AWS

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 o ID da AZ, que é um identificador exclusivo e consistente de uma zona de disponibilidade. Por exemplo, `use1-az1` é uma das zonas de disponibilidade na região `us-east-1`. Os IDs de zona de disponibilidade permitem determinar o local de recursos em uma conta em relação aos recursos em outra conta. Para obter mais informações, consulte IDs de zona de disponibilidade para recursos no Guia do usuário do AWS RAM.

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 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).

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

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.

Para identificar o proprietário de uma sub-rede (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.

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

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

Permissões de sub-redes compartilhadas

Permissões do proprietário

Os proprietários de VPCs são responsáveis por criar, gerenciar e excluir todos os recursos no nível da VPC, incluindo as sub-redes, tabelas de rotas, network ACLs, 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 gateway de trânsito.

Os proprietários de VPCs não podem modificar ou excluir os recursos de participantes que incluem grupos de segurança que os participantes criaram. Os proprietários de VPCs poderão visualizar os detalhes de todas as interfaces de rede e dos grupos de segurança que estiverem anexados aos recursos dos participantes a fim de facilitar a solução de problemas e auditoria. Os proprietários de VPCs podem criar assinaturas de log de fluxo na VPC, na sub-rede ou no nível de interface de rede para monitorar o tráfego ou solucionar problemas.

Permissões de participantes

Os participantes que estão em uma VPC compartilhada são responsáveis por criar, gerenciar e excluir seus recursos, incluindo instâncias do Amazon EC2, bancos de dados do Amazon RDS e load balancers. Os participantes não poderão visualizar ou modificar recursos que pertencerem a contas de outros participantes. Os participantes poderão visualizar detalhes das tabelas de rotas e Network ACLs que são anexadas às sub-redes compartilhadas com eles. No entanto, eles não poderão modificar recursos no nível da VPC, incluindo as tabelas de rotas, Network ACLs ou sub-redes. Os participantes poderão fazer referência aos grupos de segurança que pertencerem a outros participantes ou ao proprietário usando o ID do grupo de segurança. Os participantes só podem criar assinaturas de log de fluxo para as interfaces das quais eles são proprietários. Os participantes não podem associar diretamente uma de suas zonas hospedadas privadas à VPC compartilhada. Há duas opções se o participante precisar controlar o comportamento de uma zona hospedada privada associada à VPC:

- Os participantes podem criar e compartilhar uma zona hospedada privada com o proprietário da VPC. Para obter informações sobre como compartilhar uma zona hospedada privada, consulte Como associar uma Amazon VPC e uma zona hospedada privada que você criou com contas da AWS distintas no Guia do desenvolvedor do Amazon Route 53.
- O proprietário da VPC pode criar uma função do IAM entre contas que proporciona o controle sobre uma zona hospedada privada que o proprietário já tenha associado à VPC. O proprietário pode então conceder à conta do participante as permissões necessárias para assumir a função. Para obter mais informações, consulte Tutorial do IAM: Delegar acesso em contas da AWS usando funções do IAM no Guia do usuário do AWS Identity and Access Management. A conta de participação pode então assumir a função e exercer qualquer controle sobre a zona hospedada privada que o proprietário tenha delegado por meio da permissão da função.

Faturamento e medição para o proprietário e participantes

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 são cobrados pela transferência de dados realizadas entre zonas de disponibilidade, pela transferência de dados por conexões de emparelhamento de VPC e pela transferência de dados por um gateway do AWS Direct Connect. Os proprietários de VPCs são

cobrados por hora (quando 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. 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.

Serviços sem suporte para sub-redes compartilhadas

Os participantes não podem criar recursos para os seguintes serviços em uma sub-rede compartilhada:

- AWS CloudHSM Classic
- Amazon MQ
- Fluxos de trabalho gerenciados da Amazon para Apache Airflow (MWAA)
- RDS Proxy
- AWS Transfer Family

Um proprietário de sub-rede pode anexar um gateway de trânsito à sub-rede. Os participantes (outras contas na organização do proprietário que compartilham a sub-rede) não podem anexar o gateway de trânsito à sub-rede.

Limitações

As limitações a seguir se aplicam ao compartilhamento de VPCs:

- Os proprietários só podem compartilhar sub-redes com outras contas ou unidades organizacionais que estejam na mesma organização do AWS Organizations.
- Os proprietários não podem compartilhar sub-redes que estejam em uma VPC padrão.
- Os participantes não podem executar recursos usando grupos de segurança de propriedade de outros participantes que compartilhem a VPC ou o proprietário da VPC.
- Os participantes não podem executar recursos usando o grupo de segurança padrão da VPC, pois ele pertence ao proprietário.
- Os proprietários não podem executar recursos usando grupos de segurança de propriedade de outros participantes.
- As cotas de serviços são aplicadas por conta individual. Para obter mais informações sobre cotas de serviço, consulte Cotas de serviço da AWS na Referência geral da Amazon Web Services.
- As tags da VPC e as tags para os recursos dentro da VPC compartilhada não são compartilhadas com os participantes.
- Quando os participantes lançam recursos em uma sub-rede compartilhada, eles precisam anexar o grupo de segurança ao recurso, sem depender do grupo de segurança padrão. Os participantes não podem usar o grupo de segurança padrão, pois ele pertence ao proprietário da VPC.

Estender as VPCs

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

- As zonas de disponibilidade são vários locais isolados dentro de cada região.
- As zonas locais fornecem a capacidade de 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 datacenter, espaço de colocalização ou instalações on-premise.
- As zonas do Wavelength permitem que os desenvolvedores criem aplicativos 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 datacenters de última geração e altamente disponíveis. 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.

Para ajudar a determinar qual implantação é melhor para você, consulte Perguntas frequentes sobre o AWS Wavelength.

Estender os recursos da VPC para zonas locais

Com as AWS Local Zones, é possível se conectar facilmente a todos os serviços na região da AWS, como o Amazon Simple Storage Service e o Amazon DynamoDB por meio das mesmas APIs e conjuntos de ferramentas. É possível estender sua região da VPC criando uma nova sub-rede que tenha uma atribuição de zona local. Quando você cria uma sub-rede em uma zona local, a VPC também é estendida para essa zona local.

Para usar uma zona local, primeiro é necessário escolher a zona. Depois, crie uma sub-rede na zona local. Finalmente, inicie qualquer um dos seguintes recursos na sub-rede da zona local, para que seus aplicativos fiquem mais próximos dos usuários finais:

- Instâncias do Amazon EC2
- Volumes do Amazon EBS
- Servidores de arquivos do Amazon FSx
- Application Load Balancer
- Hosts dedicados

Um grupo de borda de rede é um conjunto exclusivo de zonas de disponibilidade ou de zonas locais de onde a AWS anuncia endereços IP públicos.

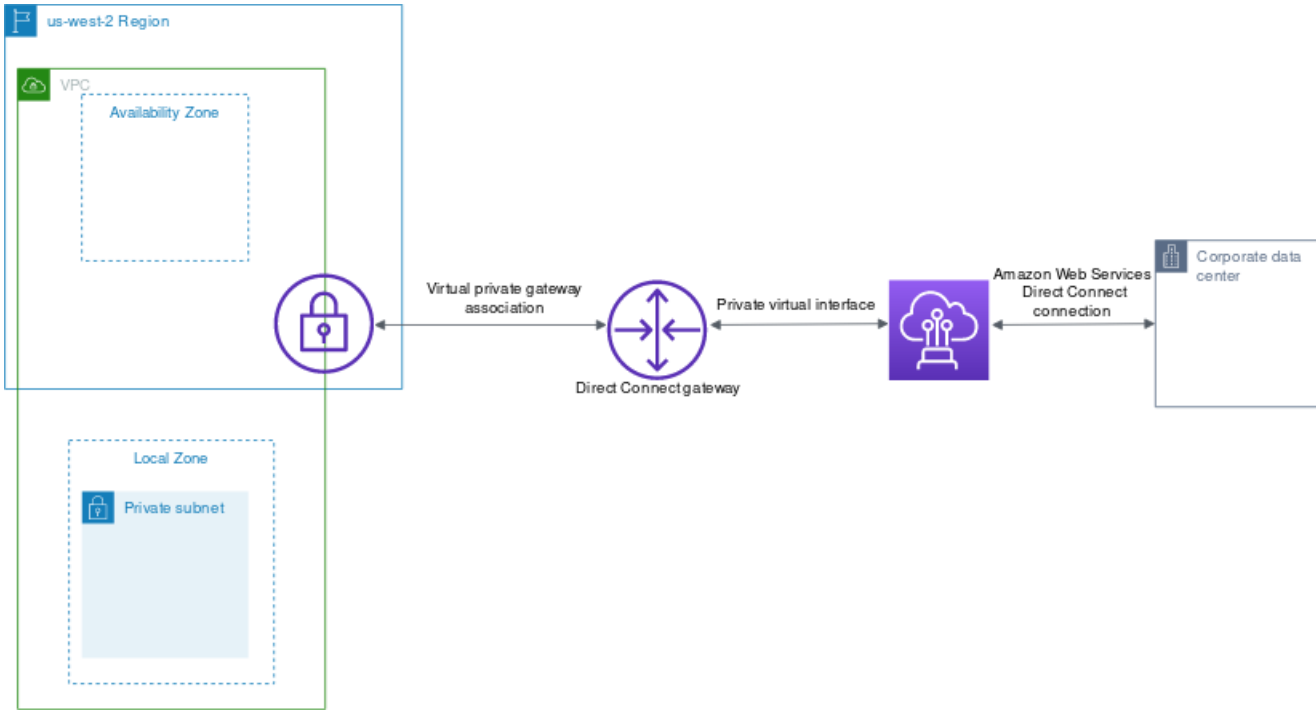
Ao criar uma VPC com endereços IPv6, é possível optar por atribuir um conjunto de endereços IP públicos fornecidos pela Amazon à VPC e também definir um grupo de borda de rede para os endereços que limita os endereços ao grupo. Ao definir um grupo de borda de rede, os endereços IP não poderão se mover entre grupos de borda de rede. O grupo de borda de rede `us-west-2` contém as quatro zonas de disponibilidade de Oeste dos EUA (Oregon). O grupo de borda de rede `us-west-2-lax-1` contém as zonas locais de Los Angeles.

As regras a seguir se aplicam às zonas locais:

- As sub-redes de zona local seguem as mesmas regras de roteamento que a sub-rede de zona de disponibilidade, incluindo tabelas de rotas, grupos de segurança e network ACLs.
- É possível atribuir zonas locais a sub-redes usando o console da Amazon VPC, a CLI da AWS ou a API.
- 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. Nós nos referimos a isso como um grupo de borda de rede e é possível definir esse parâmetro para limitar o endereço a esse local. Após provisionar os endereços IP, não será possível movê-los entre a zona local e a região pai (por exemplo, de `s-west-2-lax-1a` para `us-west-2`).
- 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.

Acessar zonas locais usando um gateway do Direct Connect

Considere o cenário em que você deseja que um datacenter on-premise 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-premise tem uma conexão do AWS Direct Connect com o local do AWS Direct Connect.



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 da sub-rede na página de detalhes da sub-rede no console da Amazon VPC ou usar describe-subnets.

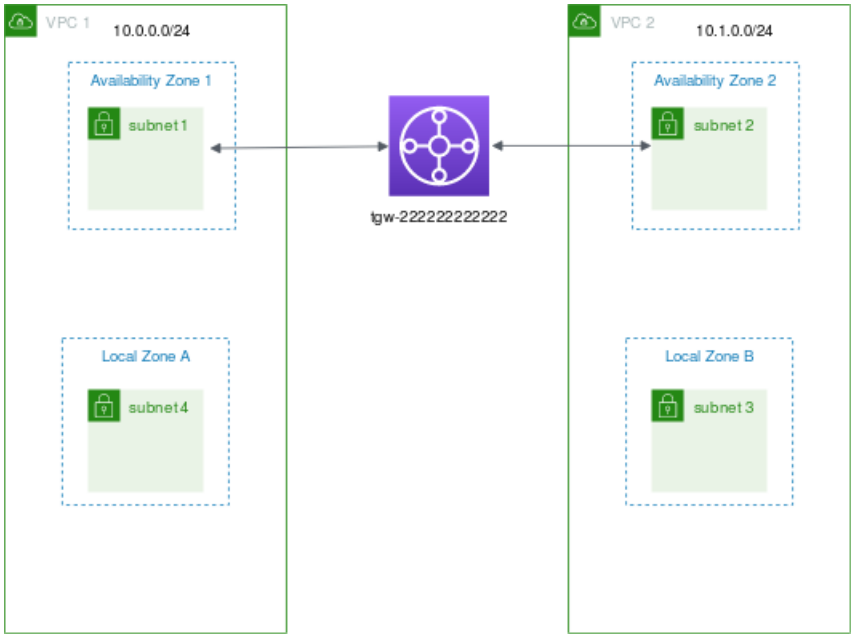
  Para obter informações sobre como criar um gateway privado virtual, consulte Criar um gateway de destino no Guia do usuário do AWS Site-to-Site VPN.
- Uma conexão do Direct Connect. A AWS recomenda que você use um dos seguintes locais para obter a melhor performance de latência para as zonas locais em LA:
  - T5 em El Segundo, Los Angeles, CA (a AWS recomenda esse local para a menor latência para a zona local em LA)
  - CoreSite LA1, Los Angeles, CA
  - Equinix LA3, El Segundo, CA

  Para obter informações sobre como solicitar uma conexão, consulte Conexões cruzadas no Guia do usuário do AWS Direct Connect.
- Gateway Direct Connect Para obter informações sobre como criar um gateway do Direct Connect, consulte Criar um gateway do Direct Connect no Guia 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 Associar e desassociar gateways privados virtuais no Guia do usuário do AWS Direct Connect.
- Uma interface virtual privada na conexão do local do AWS Direct Connect ao datacenter on-premise.

- Para obter informações sobre como criar um gateway do Direct Connect, consulte Criar uma interface virtual privada para o gateway do Direct Connect no Guia do usuário do AWS Direct Connect.

Conectar sub-redes de zona local a um gateway de trânsito

O diagrama a seguir mostra como configurar a rede para que as sub-redes na zona local se conectem a um gateway de trânsito. Você tem uma sub-rede na zona Local (sub-rede 3) e uma sub-rede na zona de disponibilidade pai (sub-rede 2). Conecte a sub-rede 2 ao gateway de trânsito e crie uma rota na tabela de rotas da VPC 2 que roteia o tráfego para o CIDR da VPC 1 para o gateway de trânsito.



É necessário criar os seguintes recursos para habilitar a comunicação:

- Uma sub-rede na zona de disponibilidade pai. Para obter informações sobre a criação de sub-redes, consulte the section called “Criar uma sub-rede na VPC” (p. 111). Use describe-availability-zones para localizar a zona pai.
- Um gateway de trânsito. Para obter informações sobre como criar um gateway de trânsito, consulte Criar um gateway de trânsito no Guia de AWS Transit Gateways.
- Um anexo da VPC para a VPC da zona de disponibilidade para o gateway de trânsito. Para obter informações sobre como criar um anexo de gateway de trânsito para uma VPC, consulte Anexos de gateways de trânsito para uma VPC no Guia de AWS Transit Gateways.
- Uma entrada para a VPC da zona de disponibilidade 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 de AWS 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” (p. 296).

  No exemplo, a tabela de rotas para a VPC 1 contém 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

Estender os recursos da VPC para zonas do Wavelength

O AWS Wavelength permite que os desenvolvedores criem aplicações 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 ampliar uma Amazon Virtual Private Cloud (VPC) para uma ou mais zonas do Wavelength e usar os recursos da AWS, como instâncias do Amazon Elastic Compute Cloud (EC2), para executar aplicativos que exigem baixíssima latência e se conectam a serviços da AWS na região.

Para usar uma zona do Wavelength, primeiro é necessário escolher a zona. Depois, 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 Roteamento no Guia do desenvolvedor do AWS Wavelength.
- É possível atribuir zonas do Wavelength a sub-redes usando o console da Amazon VPC, a CLI da AWS ou a API.
- As sub-redes nas 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 network ACLs.

Considerações sobre várias zonas de comprimento de onda

> **Note**
>
> As instâncias do EC2 que estão em duas zonas de comprimento de onda diferentes 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 de comprimento de onda.
> O tráfego entre as zonas de comprimento de onda 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 de comprimento de onda diferentes possam se comunicar. Você tem duas zonas de comprimento de onda (zona de comprimento de onda A e zona de comprimento de onda B). É necessário criar os seguintes recursos para habilitar a comunicação:

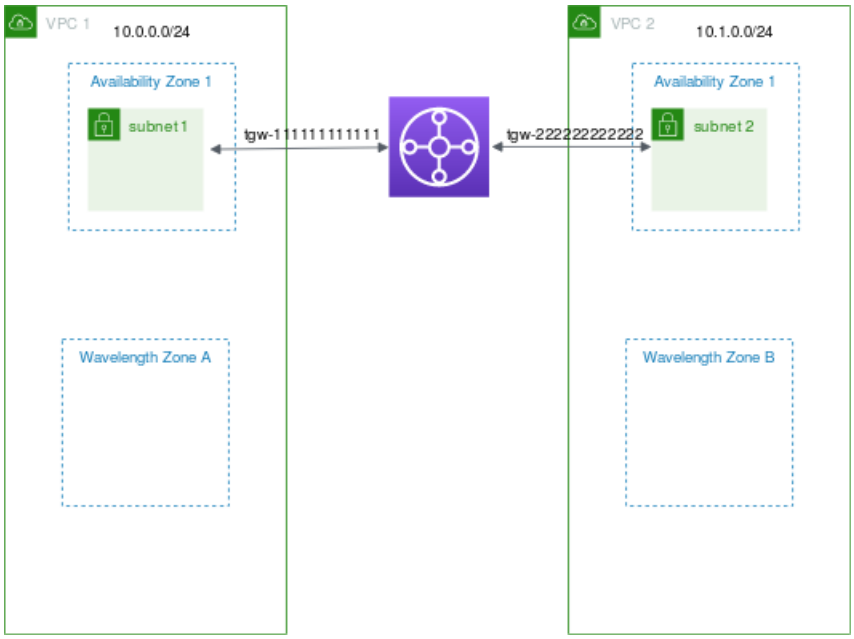
- Para cada zona de comprimento de onda, uma sub-rede em uma zona de disponibilidade pai da zona de comprimento de onda. No exemplo, você cria a sub-rede 1 e a sub-rede 2. Para obter informações sobre a criação de sub-redes, consulte the section called “Criar uma sub-rede na VPC” (p. 111). Use describe-availability-zones para localizar a zona pai.
- Um gateway de trânsito. O gateway de trânsito conecta as VPCs. Para obter informações sobre como criar um gateway de trânsito, consulte Criar um gateway de trânsito no Guia de AWS Transit Gateways.
- Para cada VPC, um anexo da VPC ao gateway de trânsito. Para obter informações sobre como criar um anexo de gateway de trânsito para uma VPC, consulte Anexos de gateways de trânsito para uma VPC no Guia de AWS Transit Gateways.
- 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 de AWS 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” (p. 296).

  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
10.1.0.0/24	tgw-22222222222222222



Sub-redes no AWS Outposts

O AWS Outposts oferece a mesma infraestrutura de hardware, serviços, APIs e ferramentas da AWS para criar e executar seus aplicativos no local e na nuvem. O AWS Outposts é ideal para cargas de trabalho que precisam de acesso de baixa latência a aplicativos ou sistemas no local e para cargas de trabalho que precisam armazenar e processar dados localmente. Para obter mais informações sobre o AWS Outposts, consulte AWS Outposts.

A Amazon VPC abrange todas as zonas de disponibilidade em uma região da AWS. Quando você conecta o Outposts à região pai, todas as VPCs existentes e recém-criadas em sua conta abrangem todas as zonas de disponibilidade e locais do Outpost associados na região.

As seguintes regras se aplicam ao AWS Outposts:

- As sub-redes devem residir em um local do Outpost.
- Um gateway local lida com a conectividade de rede entre a VPC e as redes no local. Para obter informações sobre gateways locais, consulte Gateways locais no Guia do usuário do AWS Outposts.
- Se sua conta estiver associada ao AWS Outposts, atribua a sub-rede a um Outpost especificando o ARN do Outpost ao criar a sub-rede.
- Por padrão, cada sub-rede criada em uma VPC associada a um Outpost herda a tabela de rotas da VPC principal, incluindo a rota do gateway local. Também é possível 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 que precisa ser roteado para a rede no local.

VPC e sub-redes padrão

Caso sua conta da AWS tenha sido criada após 04/12/2013, ela oferece suporte somente a EC2-VPC. Nesse caso, você terá uma VPC padrão em cada região da AWS. Uma VPC padrão está pronta para uso, portanto, você não precisa criar e configurar sua própria VPC. É possível começar a executar instâncias do Amazon EC2 imediatamente na Amazon 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 rapidamente, e para executar instâncias públicas, como um blog ou um site simples. Você pode modificar os componentes da VPC padrão conforme necessário. Se preferir criar uma VPC não padrão que atenda às suas necessidades específicas, por exemplo, para usar o intervalo de blocos CIDR e os tamanhos de sub-rede de sua preferência, consulte os cenários de exemplo (p. 80).

Tópicos

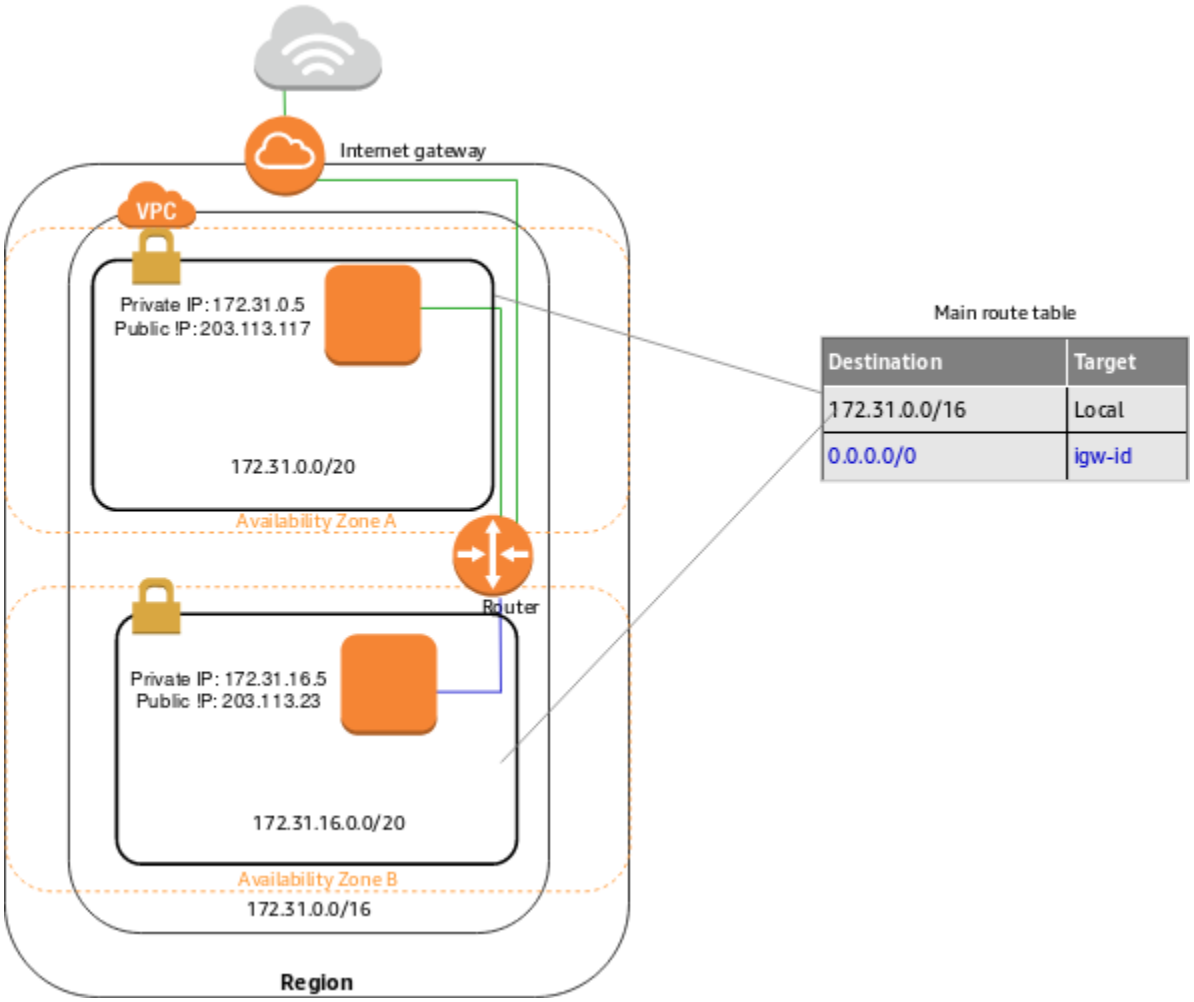
Componentes da VPC padrão

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 (p. 212) 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 de sua conta da AWS à 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.

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



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.
- Adicionar 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 de gateway Direct Connect, consulte Gateways Direct Connect no Guia 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. Para obter mais informações, Trabalhar com VPCs e sub-redes (p. 109).

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 o atributo de endereçamento IPv4 público para a sub-rede (p. 122).

De vez em quando, a AWS pode 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 obter mais informações, consulte Criar uma sub-rede padrão (p. 155).

Disponibilidade e plataformas compatíveis

Caso sua conta tenha sido criada após 04/12/2013, ela oferece suporte somente a EC2-VPC e você tem uma VPC padrão em cada região da AWS. Portanto, a menos que você crie uma VPC não padrão e especifique quando iniciar uma instância, iniciaremos suas instâncias na sua VPC padrão.

Se a conta da AWS tiver sido criada antes de 18/03/2013, ela será compatível com o EC2-Classic e o EC2-VPC nas regiões utilizadas anteriormente, mas apenas a EC2-VPC nas regiões ainda não utilizadas. Nesse caso, criamos uma VPC padrão em cada região na qual você não tenha criado nenhum recurso da AWS. A menos que você crie uma VPC não padrão e especifique-a ao executar uma instância em uma nova região, executaremos a instância na VPC padrão daquela região. No entanto, se você executar uma instância em uma região já usada antes, iniciaremos a instância em EC2-Classic.

Se você tiver criado sua conta da AWS entre 18/03/2013 e 04/12/2013, ela poderá oferecer suporte somente à EC2-VPC. Como alternativa, ela pode oferecer suporte a EC2-Classic e a EC2-VPC em algumas das regiões que você usou. Para obter mais informações sobre como detectar o suporte da plataforma em cada região para sua conta da AWS, consulte Detectar plataformas compatíveis (p. 151). Para obter mais informações sobre quando cada região foi habilitada para VPCs padrão, consulte Anúncio: habilitar as regiões para o conjunto de recursos da VPC padrão no fórum de discussão da AWS para a Amazon VPC.

Se uma conta da AWS for compatível apenas com a EC2-VPC, quaisquer contas do IAM associadas à conta da AWS também serão compatíveis somente com a EC2-VPC e usarão a mesma VPC padrão que a conta da AWS.

Se sua conta da AWS oferecer suporte a EC2-Classic e a EC2-VPC, você poderá criar uma nova conta da AWS ou executar as instâncias em uma região que você não tenha usado antes. Você pode fazer isso para obter os benefícios do uso da EC2-VPC com a simplicidade de executar instâncias no EC2-Classic. Se ainda preferir adicionar uma VPC padrão a uma região que ainda não tenha uma e que ofereça suporte a EC2-Classic, consulte "Eu realmente quero uma VPC padrão para minha conta EC2 existente. É possível?” em Perguntas frequentes sobre as VPCs padrão.

Detectar plataformas compatíveis

É possível usar o console do Amazon EC2 ou a linha de comando para determinar se sua conta da AWS é compatível com as duas plataformas, ou se você tem uma VPC padrão.

Como detectar o suporte para a plataforma usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, use o seletor de região no canto superior direito para selecionar a região.
3. No painel do Console do Amazon EC2, procure Supported Platforms (Plataformas com suporte) em Account Attributes (Atributos da conta). Se houver dois valores, `EC2` e `VPC`, é possível executar instâncias em qualquer uma das plataformas. Se houver um único valor `VPC`, somente é possível executar instâncias em EC2-VPC.

   O seguinte exemplo indica que a conta oferece suporte somente para a plataforma EC2-VPC e tem uma VPC padrão com o identificador `vpc-1a2b3c4d`.

   Ao excluir sua VPC padrão, o valor Default VPC exibido será `None`.

Para detectar o suporte para a plataforma usando a linha de comando

- describe-account-attributes (CLI da AWS)
- Get-EC2AccountAttribute (AWS Tools for Windows PowerShell)

O atributo `supported-platforms` na saída indica em quais plataformas você pode executar instâncias do EC2.

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.

Como visualizar a VPC e as sub-redes padrão 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 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 o describe-vpcs (CLI da AWS)
- Use o 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 o describe-subnets (CLI da AWS)
- Use o 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.

Executar uma instância do EC2 na VPC padrão

Ao iniciar uma instância do EC2 sem especificar uma sub-rede, ela é automaticamente iniciada em uma sub-rede padrão na sua VPC padrão. Por padrão, selecionamos uma zona de disponibilidade e iniciamos a instância na sub-rede correspondente a essa zona de disponibilidade. Como alternativa, é possível selecionar a zona de disponibilidade para a instância selecionando a sub-rede padrão correspondente no console ou especificando a sub-rede ou a zona de disponibilidade na CLI da AWS.

Executar uma instância do EC2 usando o console

Para iniciar uma instância do EC2 na VPC padrão

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel do EC2, escolha Launch Instance.
3. Siga as orientações no assistente. Selecione uma AMI e escolha um tipo de instância. Você pode aceitar as configurações padrão para o restante do assistente escolhendo Review and Launch. Isso conduzirá você diretamente para a página Review Instance Launch.
4. Revise suas configurações. Na seção Instance Details, o padrão para Subnet é No preference (default subnet in any Availability Zone). Isso significa que a instância é iniciada na sub-rede padrão da zona de disponibilidade que selecionamos. Alternativamente, escolha Edit instance details e selecione a sub-rede padrão para uma zona de disponibilidade específica.
5. Escolha Launch para escolher um par de chaves e iniciar a instância.

Executar uma instância do EC2 usando a linha de comando

Você pode usar um dos seguintes comandos para iniciar uma instância do EC2:

- run-instances (CLI da AWS)
- New-EC2Instance (AWS Tools for Windows PowerShell)

Para iniciar uma instância do EC2 em sua VPC padrão, use esses comandos sem especificar uma sub-rede ou uma zona de disponibilidade.

Para iniciar uma instância do EC2 em uma sub-rede padrão específica em sua VPC padrão, especifique o ID da sub-rede ou a zona de disponibilidade.

Excluir suas sub-redes e VPC padrão

É possível excluir uma sub-rede padrão ou uma VPC padrão, assim como qualquer outra sub-rede ou VPC. Para obter mais informações, consulte Trabalhar com VPCs e sub-redes (p. 109). No entanto, ao

excluir suas sub-redes padrão ou VPC padrão, é preciso especificar explicitamente uma sub-rede em outra VPC para iniciar a instância, porque você não poderá iniciar as instâncias no EC2-Classic. Se você não tiver outra VPC, será preciso criar uma VPC não padrão e uma sub-rede não padrão. Para obter mais informações, consulte Criar uma VPC (p. 110).

Se excluir a VPC padrão, você poderá criar uma nova. Para obter mais informações, consulte Criar uma VPC padrão (p. 154).

Se excluir uma sub-rede padrão, você poderá criar uma nova. Para obter mais informações, consulte Criar uma sub-rede padrão (p. 155). Como alternativa, você pode criar uma sub-rede não padrão na sua VPC padrão e entrar em contato com o AWS Support para marcar a sub-rede como sub-rede padrão. É necessário fornecer os seguintes detalhes: o ID da sua conta da AWS, a região e o ID da sub-rede. 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 o atributo de endereçamento IPv4 público para a sub-rede (p. 122). 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.

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. Se sua conta oferecer suporte a EC2-Classic, você não poderá usar estes procedimentos para criar uma VPC padrão em uma região que ofereça suporte a EC2-Classic.

Quando você cria uma VPC padrão, ela é criada com os componentes (p. 149) 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.

Como criar uma VPC padrão 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 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 CLI da AWS. Esse comando não tem nenhum parâmetro de entrada.

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

```
{
    "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 das Ferramentas para Windows PowerShell ou a ação CreateDefaultVpc da API do Amazon EC2.

Criar uma sub-rede padrão

Você pode criar uma sub-rede padrão em uma zona de disponibilidade que não tenha uma. Por exemplo, é recomendável criar uma sub-rede padrão caso a sub-rede padrão tenha sido excluída ou a AWS tenha adicionado uma nova zona de disponibilidade e não tenha 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 (p. 104).

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 obter mais informações, consulte Associar um bloco CIDR IPv6 à sub-rede (p. 114).

Atualmente, é possível criar uma sub-rede padrão usando apenas a CLI da AWS, um AWS SDK ou a API do Amazon EC2.

Como criar uma sub-rede padrão usando a CLI da AWS

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

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

```
{
    "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 como configurar a CLI da AWS, consulte o Guia do usuário da interface de linha de comando da AWS.

Como alternativa, é possível usar o comando New-EC2DefaultSubnetdas Ferramentas para Windows PowerShell ou a ação CreateDefaultSubnet da API do Amazon EC2.

Segurança na Amazon Virtual Private Cloud (VPC)

A segurança da nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você aproveita um datacenter e uma arquitetura de rede criados para atender aos requisitos das empresas 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 por proteger a infraestrutura que executa serviços da AWS na Nuvem AWS. A AWS também fornece serviços que você pode usar com segurança. Auditores externos 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: a responsabilidade é determinada pelo serviço da AWS usado. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da sua 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.

Tópicos

Proteção de dados na Amazon Virtual Private Cloud

O modelo de responsabilidade compartilhada da AWS se aplica à proteção de dados na AWS 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 seu conteúdo hospedado nessa infraestrutura. Esse conteúdo inclui as tarefas de configuração e gerenciamento de segurança dos serviços da AWS que você usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para obter mais informações sobre a proteção de dados na Europa, consulte o blog Responsabilidade compartilhada da AWS e GDPR no Blog de segurança da AWS.

Para fins de proteção de dados, recomendamos que você proteja as credenciais da conta da AWS e configure contas de usuário individuais com o 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. Recomendamos TLS 1.2 ou posterior.
- Configure o registro em log de atividades da API e do usuário com o AWS CloudTrail.
- Use as soluções de criptografia da AWS, juntamente com todos os controles de segurança padrão nos serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados pessoais armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar a AWS por meio de uma interface de linha de comando ou uma API, use um endpoint do FIPS. Para obter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que você nunca coloque informações de identificação confidenciais, como números de conta dos seus clientes, em campos de formato livre, como um campo Name (Nome). Isso inclui quando você trabalhar com a AWS VPC ou outros serviços da AWS usando o console, a API, a CLI da AWS ou os AWS SDKs. Todos os dados inseridos na AWS VPC ou em outros serviços poderão ser selecionados para inclusão em logs de diagnóstico. Ao fornecer um URL para um servidor externo, não inclua informações de credenciais no URL para validar a solicitação a esse servidor.

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: atuam como firewall para instâncias associadas do Amazon EC2, controlando o tráfego de entrada e de saída no nível da instância. Ao executar uma instância em uma VPC, você pode associar um ou mais grupos de segurança que criar. Cada instância na VPC pode pertencer a um conjunto diferente de grupos de segurança. Se você não especificar um grupo de segurança ao executar uma instância, ela será associada automaticamente ao grupo de segurança padrão da VPC. Para obter mais informações, consulte Grupos de segurança para a VPC (p. 180).
- Listas de controles de acesso à rede (ACLs): as Network ACLs funcionam como firewall para sub-redes associadas, controlando o tráfego de entrada e de saída no nível da sub-rede. Para obter mais informações, consulte Network ACLs (p. 190).
- 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 Network ACL e grupos de segurança excessivamente restritivos ou permissivos. Para obter mais informações, consulte VPC Flow Logs (p. 310).
- 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.

É possível usar o AWS Identity and Access Management (IAM) para controlar quem na organização tem permissão para criar e gerenciar grupos de segurança, Network ACLs e logs de fluxo. Por exemplo, você pode conceder essa permissão aos administradores da rede, mas não conceder permissão ao pessoal que só precisa executar instâncias. Para obter mais informações, consulte Identity and Access Management para o Amazon VPC (p. 162).

Os grupos de segurança e as Network ACLs da Amazon não filtram o tráfego destinado aos seguintes serviços da Amazon nem proveniente deles:

- Serviços de nomes de domínio (DNS) da Amazon

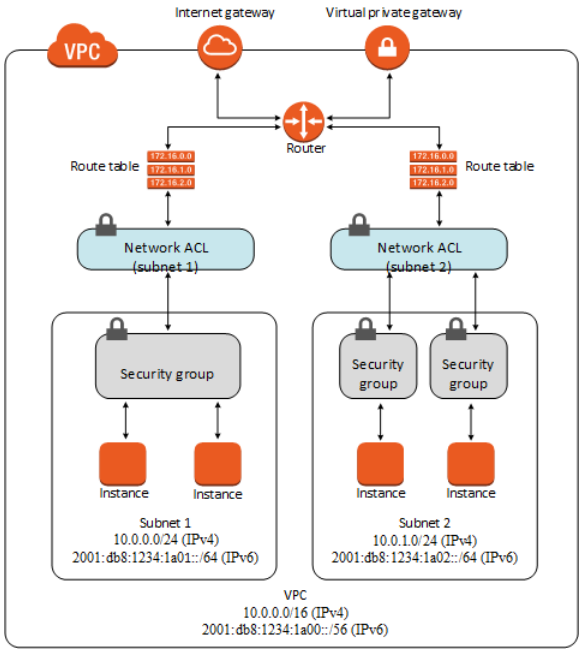
- Dynamic Host Configuration Protocol (DHCP – Protocolo de configuração de host dinâmico) da Amazon
- Metadados da instância do Amazon EC2
- Ativação de licença do Windows da Amazon
- Amazon Time Sync Service
- Endereço IP reservado do roteador padrão da VPC

Comparação entre grupos de segurança e network ACLs

A tabela a seguir resume as diferenças básicas entre grupos de segurança e Network ACLs.

Grupo de segurança	Network ACL
Opera em nível de instância	Opera em nível de sub-rede
Comporta apenas regras de permissão	Comporta regras de permissão e negação
É stateful: o tráfego de retorno é permitido automaticamente, seja qual for a regra	É stateless: o tráfego de deve ser permitido explicitamente pelas regras
Avaliamos todas as regras antes de decidir se permitimos ou não o tráfego	Processamos regras em ordem, começando com a regra de número menor, ao decidir se deve permitir o tráfego
Aplica-se a uma instância somente se alguém especificar o security group ao executar uma instância ou associa posteriormente o security group com a instância	Aplica-se automaticamente a todas as instâncias nas sub-redes com as quais está associada (portanto, fornece uma camada adicional de defesa, caso as regras do grupo de segurança sejam permissivas demais)

O diagrama a seguir mostra as camadas de segurança fornecidas por grupos de segurança e Network ACLs. 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 Network ACL 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 Network ACLs como uma camada adicional de defesa. Para ver um exemplo, consulte Exemplo: Controlar o acesso a instâncias em uma sub-rede (p. 207).

Criptografia em trânsito

A AWS fornece conectividade privada e segura entre instâncias do EC2 de todos os tipos. Além disso, alguns tipos de instância usam os recursos de descarregamento do hardware subjacente para criptografar automaticamente o tráfego em trânsito entre instâncias, usando algoritmos AEAD com criptografia de 256 bits. Não há impacto no desempenho da rede. Para obter mais informações sobre a criptografia de instâncias, consulte Criptografia em trânsito no Guia do usuário do Amazon EC2 para instâncias do Linux.

Segurança da infraestrutura no Amazon S3

Como um serviço gerenciado, a Amazon VPC é protegida pelos procedimentos de segurança da rede global da AWS descritos no whitepaper Amazon Web Services: visão geral dos processos de segurança.

Você usa as chamadas de API da AWS para acessar a Amazon VPC por meio da rede. Os clientes devem oferecer suporte a Transport Layer Security (TLS) 1.0 ou posterior. Recomendamos TLS 1.2 ou posterior. Os clientes também devem ter suporte a pacotes de criptografia com sigilo de encaminhamento perfeito (PFS) como Ephemeral Diffie-Hellman (DHE) ou Ephemeral Elliptic Curve Diffie-Hellman (ECDHE). A maioria dos sistemas modernos como Java 7 e versões posteriores oferece suporte a 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 você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Isolamento de rede

Uma nuvem privada virtual (VPC) é uma rede virtual em sua própria área isolada logicamente na Nuvem AWS. Use VPCs separadas para isolar a infraestrutura por carga de trabalho 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 seu aplicativo (por exemplo, Web, aplicativo e banco de dados) em uma única VPC. Use sub-redes privadas para as instâncias que não devem ser acessadas diretamente pela Internet.

Para chamar a API do Amazon EC2 da VPC sem enviar tráfego pela Internet pública, use o AWS PrivateLink.

Controlar o tráfego de rede

Considere as seguintes opções de controle de tráfego de rede para suas instâncias do EC2:

- Restrinja o acesso às sub-redes usando the section called “Grupos de segurança” (p. 180). Por exemplo, você pode permitir tráfego apenas de intervalos de endereços de sua rede corporativa.
- Use os grupos de segurança como o mecanismo primário a fim de controlar o acesso à rede para instâncias das VPCs. Quando necessário, use as 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. No entanto, as ACLs de rede podem ser eficientes como um controle secundário para negar um subconjunto ou tráfego específico ou fornecer grades de proteção de sub-rede de alto nível. Além disso, como as ACLs de rede se aplicam a toda uma sub-rede, elas podem ser usadas como defesa em profundidade caso uma instância seja iniciada de forma não intencional 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 acesso à Internet em uma instância em uma sub-rede privada.
- Configure as tabelas de rotas de sub-rede da Amazon VPC com as rotas de rede mínimas necessárias. Por exemplo, insira somente as instâncias do Amazon EC2 que exigem acesso direto à Internet nas sub-redes com rotas para um gateway da Internet e insira somente instâncias do Amazon EC2 que precisem de acesso direto a redes internas nas sub-redes com rotas para um gateway privado virtual.
- 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. Esta abordagem permite que os clientes implementem políticas do IAM especiais para o 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 a AWS Virtual Private Network ou o AWS Direct Connect para estabelecer conexões privadas das redes remotas com as VPCs. Para obter mais informações, consulte 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.

Além de restringir o acesso à rede para cada instância do Amazon EC2, a Amazon VPC é compatível com a implementação de controles de segurança de rede adicionais, como gateways em linha, servidores de proxy e várias opções de monitoramento de rede.

Para obter mais informações, consulte o whitepaper Práticas recomendadas de segurança da AWS.

Identity and Access Management para o Amazon VPC

O AWS Identity and Access Management (IAM) é um serviço da AWS que ajuda um administrador a controlar de forma segura 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 serviço da AWS que pode ser usado sem custo adicional.

Tópicos

Público

A maneira como você usa o AWS Identity and Access Management (IAM) muda de acordo com o 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 (p. 176).

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 (p. 166).

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 (p. 170).

Autenticar com identidades

A autenticação é a forma como você faz login na AWS usando suas credenciais de identidade. Para obter mais informações sobre como fazer login usando o Console de Gerenciamento da AWS, consulte Fazer login no Console de Gerenciamento da AWS como usuário do IAM ou usuário raiz no Guia do usuário do IAM.

É necessário estar autenticado (conectado à AWS) como o usuário raiz da conta da AWS, um usuário do IAM ou assumindo uma função do IAM. Também é possível usar a autenticação de logon único da sua empresa ou até mesmo fazer login usando o Google ou o Facebook. Nesses casos, o administrador configurou anteriormente federação de identidades usando funções do IAM. Ao acessar a AWS usando credenciais de outra empresa, você estará assumindo uma função indiretamente.

Para fazer login diretamente no Console de Gerenciamento da AWS, use sua senha com o e-mail do usuário raiz ou com o nome do usuário do IAM. É possível acessar a AWS de maneira programática usando o usuário raiz ou as chaves de acesso dos usuários do IAM. A AWS fornece o SDK e as ferramentas da linha de comando para assinar de forma criptográfica sua solicitação usando suas credenciais. Se você não utilizar ferramentas da AWS, cadastre a solicitação você mesmo. Faça isso usando o Signature versão 4, um protocolo para autenticação de solicitações de API de entrada. Para obter mais informações sobre solicitações de autenticação, consulte Processo de assinatura do Signature versão 4 na Referência geral da AWS.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, a AWS recomenda o uso de autenticação multifator (MFA) para aumentar a segurança de conta. Para saber mais, consulte Usar Multi-Factor Authentication (MFA) na AWS no Guia do usuário do IAM.

Usuário raiz da conta da AWS

Ao criar uma conta do AWS pela primeira vez, você começa com uma única identidade de login que tem acesso completo a todos os serviços e recursos da AWS na conta. Essa identidade é denominada usuário raiz da conta da AWS e é acessada pelo login com o endereço de e-mail e a senha que você usou para criar a conta. Recomendamos que não use o usuário raiz para suas tarefas diárias, nem mesmo as administrativas. Em vez disso, siga as práticas recomendadas para o uso do usuário raiz somente a fim de criar seu primeiro usuário do IAM. Depois, armazene as credenciais do usuário raiz com segurança e use-as para executar somente algumas tarefas de gerenciamento de contas e de serviços.

Grupos e usuários do IAM

Um usuário do IAM é uma identidade em sua conta da AWS que tem permissões específicas para uma única pessoa ou uma única aplicação. Um usuário do IAM pode ter credenciais de longo prazo, como um nome de usuário e uma senha ou um conjunto de chaves de acesso. Para saber como gerar chaves de acesso, consulte Gerenciar chaves de acesso para usuários do IAM no Guia do usuário do IAM. Ao gerar chaves de acesso para um usuário do IAM, visualize e salve o par de chaves de maneira segura. Não será possível recuperar a chave de acesso secreta futuramente. Em vez disso, você deverá gerar outro par de chaves de acesso.

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 atribuir a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de funções. Um usuário é exclusivamente associado a uma pessoa ou a um aplicativo, mas uma função pode ser assumida por qualquer pessoa que precisar dela. Os usuários têm credenciais permanentes de longo prazo, mas as funções fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de uma função) no Guia do usuário do IAM.

Funções do IAM

Uma função do IAM é uma identidade dentro da sua conta da AWS que tem permissões específicas. Ela é semelhante a um usuário do IAM, mas não está associada a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no Console de Gerenciamento da AWS alternando funções. É possível assumir uma função chamando uma operação de API da AWS ou uma CLI da AWS ou usando um URL personalizado. Para mais informações sobre métodos para o uso de funções, consulte Usar funções do IAM no Guia do usuário do IAM.

As funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- Permissões temporárias para usuários do IAM: um usuário do IAM pode assumir uma função do IAM para obter temporariamente permissões diferentes para uma tarefa específica.

- Acesso de usuário federado: em vez de criar um usuário do IAM, é possível usar identidades existentes do AWS Directory Service, o diretório de usuários da sua empresa ou um provedor de identidades da web. Estes são conhecidos como usuários federados. A AWS atribui uma função a um usuário federado quando o acesso é solicitado por meio de um provedor de identidades. Para obter mais informações sobre usuários federados, consulte Usuários federados e funções no Guia do usuário do IAM.
- Acesso entre contas: é possível usar uma função do IAM para permitir que alguém (um principal confiável) em outra conta acesse recursos em sua conta. As funções são a principal forma de conceder acesso entre contas. No entanto, com alguns serviços da AWS, é possível anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recurso para acesso entre contas, consulte Como as funções do IAM diferem das políticas baseadas em recurso 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 do principal de chamada, usando uma função de serviço ou uma função vinculada ao serviço.
  - Permissões principais: quando você usa um usuário ou uma função do IAM para executar ações na AWS, você é considerado um principal. As políticas concedem permissões a uma entidade principal. Quando você usa alguns serviços, pode executar uma ação que, em seguida, aciona outra ação em outro serviço. Nesse caso, você deve ter permissões para executar ambas as ações. Para ver se uma ação requer ações dependentes adicionais em uma política, consulte Ações, recursos e chaves de condição para o Amazon Elastic Compute Cloud na Referência de autorização do serviço.
  - Função de serviço: uma função de serviço é uma função do IAM que um serviço assume para realizar ações em seu nome. As funções de serviço fornecem acesso apenas dentro de sua conta e não podem ser usadas para conceder acesso a serviços em outras contas. Um administrador do IAM pode criar, modificar e excluir uma função de serviço do IAM. Para obter mais informações, consulte Criar uma função para delegar permissões a um serviço da AWS no Guia do usuário do IAM.
  - Função vinculada ao serviço: uma função vinculada ao serviço é um tipo de função de serviço vinculada a um serviço da AWS. O serviço pode assumir a função de executar uma ação em seu nome. As funções vinculadas ao 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.
- Aplicações em execução no Amazon EC2: é possível usar uma função do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 que fazem solicitações da API ou da CLI da AWS. É preferível fazer isso do que armazenar chaves de acesso na instância do EC2. Para atribuir uma função da AWS a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, crie um perfil de instância para ser anexado à instância. Um perfil de instância contém a função e permite que programas que estão em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar uma função do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar as funções do IAM, consulte Quando criar uma função do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciamento do acesso usando políticas

Você controla o acesso na AWS criando políticas e anexando-as às identidades do IAM ou aos recursos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou a um recurso, define suas permissões. Você pode fazer login como o usuário raiz ou um usuário do IAM ou assumir uma função do IAM. Quando você faz uma solicitação, a AWS avalia as políticas relacionadas baseadas em identidade ou baseadas em recursos. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas são armazenadas 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 a quê. Ou seja, qual principal pode executar ações em quais recursos, e em que condições.

Cada entidade do IAM (usuário ou função) começa sem permissões. Em outras palavras, por padrão, os usuários não podem fazer nada, nem mesmo alterar sua própria senha. Para dar permissão a um usuário para fazer algo, um administrador deve anexar uma política de permissões ao usuário. Ou o administrador pode adicionar o usuário a um grupo que tenha as permissões pretendidas. Quando um administrador concede permissões a um grupo, todos os usuários desse grupo recebem essas permissões.

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 da função no Console de Gerenciamento da AWS, na CLI da AWS ou na API da 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 função do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou função. As políticas gerenciadas são políticas independentes que podem ser anexadas a vários usuários, grupos e funções em sua 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 recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de função 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 recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar um principal em uma política baseada em recursos. Os principais podem incluir contas, usuários, funções, usuários federados ou serviços da AWS.

Políticas baseadas em recursos são políticas em linha que estão localizadas nesse serviço. Você não pode usar as políticas gerenciadas da AWS do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais principais (membros, usuários ou funções 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 suporte a 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 suporte a outros 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 função do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade da entidade e seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou a função 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 o máximo de permissões para uma organização ou unidade organizacional (UO) no AWS Organizations. O AWS Organizations é um serviço para agrupar e gerenciar centralmente várias contas da AWS que sua empresa possui. 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-membro, incluindo cada usuário raiz da conta da AWS. Para mais informações sobre organizações e SCPs, consulte Como as SCPs funcionam 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 uma função ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou da função e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recurso. 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 vários tipos de política estão envolvidos, consulte Lógica de avaliação de políticas no Guia 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 que funcionam 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 conhecer 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 principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política 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. Há também algumas operações que 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 alguém para criar uma VPC com a operação `CreateVpc` da API do Amazon EC2, inclua a ação `ec2:CreateVpc` na política da pessoa. 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 da Amazon VPC, consulte Ações, recursos e chaves de condição do Amazon EC2 no Guia do usuário do IAM.

Recursos

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

O elemento `Resource` de política JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou um elemento `NotResource`. Como prática recomendada, especifique um recurso usando seu Nome de recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem suporte a um tipo de recurso específico, conhecido como permissões em nível de recurso.

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

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

> **Important**
>
> No momento, nem todas as ações de API do Amazon EC2 são compatíveis com permissões em nível de recurso. Se uma ação da API do Amazon EC2 não oferecer suporte a permissões em nível de recurso, você poderá conceder aos usuários permissão para usar a ação, mas precisará especificar um * para o elemento do recurso da declaração de política. Para exibir as ações para as quais você pode especificar um ARN para o elemento de recurso, consulte Ações definidas pelo Amazon EC2.

O recurso da VPC tem o ARN exibido no exemplo a seguir.

```
arn:${Partition}:ec2:${Region}:${Account}:vpc/${VpcId}
```

Para obter mais informações sobre o formato de ARNs, consulte Nomes de recursos da Amazon (ARNs).

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 instrução, separe os ARNs com vírgulas.

```
"Resource": [
      "resource1",
      "resource2"
]
```

Para ver uma lista dos tipos de recursos da Amazon VPC e seus ARNs, consulte Recursos definidos pelo Amazon EC2 no Guia do usuário do IAM.

Chaves de condição

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

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

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único elemento `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 para que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar as 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 de política do IAM: variáveis e tags no Guia do usuário do IAM.

A AWS oferece suporte a chaves de condição globais e chaves de condição específicas do serviço. Para conhecer todas as chaves de condição globais da AWS, consulte Chaves de contexto de condição globais da AWS no Guia do usuário do IAM.

A Amazon VPC define seu próprio conjunto de chaves de condição e também oferece suporte ao uso de algumas chaves de condição globais. Para conhecer 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: restrição de acesso a uma região específica.

Para ver uma lista de chaves de condição da Amazon VPC, consulte Chaves de condição para o Amazon EC2 no Guia do usuário do IAM. Para saber com quais ações e recursos você pode 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 um 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 um principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para mais informações, consulte Como as funções do IAM diferem de políticas baseadas em recursos 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 baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as chaves de condição `ec2:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`. Para obter mais informações, consulte Permissões no nível do recurso para marcação no Guia do usuário do Amazon EC2.

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 (p. 175).

Funções do IAM

Uma função do IAM é uma entidade dentro de 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

Funções vinculadas ao serviço permitem que os serviços da AWS acessem recursos em outros serviços para concluir uma ação em seu nome. As funções vinculadas ao 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 recurso permite que um serviço assuma uma função de serviço em seu nome. A função permite que o serviço acesse recursos em outros serviços para concluir uma ação em seu nome. As funções 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 essa função. 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 obter mais informações, consulte Funções do IAM para publicar logs de fluxo no CloudWatch Logs (p. 322).

Exemplos de políticas da Amazon VPC

Por padrão, os usuários e as funções do IAM não têm permissão para criar ou modificar recursos da VPC. Eles também não podem executar tarefas usando o Console de Gerenciamento da AWS, a CLI da AWS ou a API da AWS. Um administrador do IAM deve criar políticas do IAM que concedam aos usuários e funções permissão para executarem operações de API específicas nos recursos especificados de que precisam. O administrador deve anexar essas políticas aos usuários ou grupos do IAM que exigem essas permissões.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documentos de política JSON, consulte Criar políticas na guia JSON no Guia do usuário do IAM.

Tópicos

Melhores práticas de políticas

As políticas baseadas em identidade são muito eficientes. Elas determinam se alguém pode criar, acessar ou excluir recursos do 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:

- Começar a usar políticas gerenciadas pela AWS: para começar a usar a Amazon VPC rapidamente, use políticas gerenciadas pela AWS para conceder aos funcionários as permissões de que eles precisam. Essas políticas já estão disponíveis em sua conta e são mantidas e atualizadas pela AWS. Para obter mais informações, consulte Começar a usar permissões com políticas gerenciadas pela AWS no Guia do usuário do IAM.
- Conceder privilégio mínimo: ao criar políticas personalizadas, conceda apenas as permissões necessárias para executar uma tarefa. Comece com um conjunto mínimo de permissões e conceda permissões adicionais conforme necessário. Fazer isso é mais seguro do que começar com permissões

que são muito lenientes e tentar restringi-las posteriormente. Para obter mais informações, consulte Conceder privilégio mínimo no Guia do usuário do IAM.

- Habilitar MFA para operações confidenciais: para aumentar a segurança, exija que os usuários do IAM usem Multi-Factor Authentication (MFA) para acessar recursos ou operações de API confidenciais. Para obter mais informações, consulte Usar Multi-Factor Authentication (MFA) na AWS no Guia do usuário do IAM.
- Usar condições de política para segurança adicional: na medida do possível, defina as condições sob as quais suas políticas baseadas em identidade permitem o acesso a um recurso. Por exemplo, você pode gravar condições para especificar um intervalo de endereços IP permitidos do qual a solicitação deve partir. Você também pode escrever condições para permitir somente solicitações em uma data especificada ou período ou para exigir o uso de SSL ou MFA. Para obter mais informações, consulte Elementos de política JSON do IAM: condição no Guia do usuário do IAM.

Visualizar 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 (usuários ou funções do IAM) com essa política.

A política a seguir concede permissão aos usuários 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: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 os usuários que estão fazendo ligações somente com a CLI da AWS ou a API da AWS. Em vez disso, para esses usuários, permita o acesso somente às ações que correspondam à operação da API que precisam executar.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou de forma programática usando a CLI da AWS ou a API da AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Criar uma VPC com uma sub-rede pública

O exemplo a seguir permite que os usuários criem VPCs, sub-redes, tabelas de rota e gateways da Internet. Os usuários também podem anexar um gateway da Internet a uma VPC e criar rotas em tabelas de rotas. A ação `ec2:ModifyVpcAttribute` permite que os usuários 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 usuários criem uma VPC usando a primeira opção de configuração do assistente da VPC no console da Amazon VPC. Para exibir o assistente da VPC, os usuários também devem ter permissão para usar o `ec2:DescribeVpcEndpointServices`. Isso garante que a seção de VPC endpoints do assistente da VPC seja carregada corretamente.

Modificar e excluir recursos da VPC

É possível controlar quais recursos da VPC os usuários podem modificar ou excluir. Por exemplo, a política a seguir permite que os usuários trabalhem com e excluam tabelas de rotas com a tag `Purpose=Test`. A política também especifica que os usuários podem excluir somente os gateways da Internet que tenham a tag `Purpose=Test`. Os usuários não podem trabalhar com tabelas de rota ou gateways da Internet que não tenham essa tag.

```
{
    "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 concede permissão aos usuários para criar e excluir regras de entrada e de saída para qualquer security group de uma VPC específica. A política faz isso, aplicando uma chave de condição (`ec2:Vpc`) ao recurso do security group para as ações `Authorize` e `Revoke`.

A segunda instrução concede permissão aos usuários para descrever todos os security groups. Isso permite que os usuários visualizem as regras de grupo de segurança a fim de modificá-las.

```
{
"Version": "2012-10-17",
  "Statement":[{
    "Effect":"Allow",
    "Action": [
       "ec2:AuthorizeSecurityGroupIngress",
       "ec2:AuthorizeSecurityGroupEgress",
       "ec2:RevokeSecurityGroupIngress",
       "ec2:RevokeSecurityGroupEgress"],
     "Resource": "arn:aws:ec2:region:account:security-group/*",
      "Condition": {
        "ArnEquals": {
          "ec2:Vpc": "arn:aws:ec2:region:account:vpc/vpc-11223344556677889"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeSecurityGroups",
      "Resource": "*"
    }
  ]
}
```

Para visualizar grupos de segurança na página Security Groups (Grupos de segurança) do console da Amazon VPC, os usuários devem ter permissão para usar a ação `ec2:DescribeSecurityGroups`. Para usar a página Create security group (Criar grupo de segurança), os usuários devem ter permissões para usar as ações `ec2:DescribeVpcs` e `ec2:CreateSecurityGroup`.

A política a seguir permite que os usuários visualizem e criem grupos de segurança. Também permite que adicionem e removam regras de entrada e saída de qualquer grupo de segurança que esteja associado a `vpc-11223344556677889`.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeSecurityGroups", "ec2:DescribeVpcs", "ec2:CreateSecurityGroup"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteSecurityGroup", "ec2:AuthorizeSecurityGroupIngress",
 "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress", "ec2:RevokeSecurityGroupEgress"
      ],
```

```
      "Resource": "arn:aws:ec2:*:*:security-group/*",
      "Condition":{
         "ArnEquals": {
            "ec2:Vpc": "arn:aws:ec2:*:*:vpc/vpc-11223344556677889"
         }
      }
    }
   ]
}
```

Para permitir que os usuários alterem o grupo de segurança associado a uma instância, adicione a ação `ec2:ModifyInstanceAttribute` à sua política. Como alternativa, para permitir que os usuários alterem grupos de segurança de uma interface de rede, adicione a ação `ec2:ModifyNetworkInterfaceAttribute` à sua política.

Executar instâncias em uma sub-rede específica

A política a seguir concede permissões aos usuários para executarem instâncias em uma sub-rede específica e usarem um security group específico na solicitação. A política faz isso, especificando o ARN para `subnet-11223344556677889` e o ARN para `sg-11223344551122334`. Se usuários tentarem executar uma instância em uma sub-rede diferente ou usar um security group diferente, haverá falha na solicitação (a menos que outra política ou instrução conceda aos usuários 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 usuário precise de permissão para criar esse recurso quando 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-11223344556677889",
        "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-11223344551122334"
      ]
    }
   ]
}
```

Executar instâncias em uma VPC específica

A política a seguir concede permissões aos usuários para executarem 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 usuários de executarem instâncias usando somente AMIs que possuam a tag "`department=dev`".

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:region:account:subnet/*",
```

```
        "Condition": {
         "StringEquals": {
            "ec2:Vpc": "arn:aws:ec2:region:account:vpc/vpc-11223344556677889"
            }
      }
   },
   {
      "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/*"
         ]
      }
   ]
}
```

Exemplos adicionais de políticas da Amazon VPC

É possível encontrar políticas de exemplo do IAM adicionais relacionadas à Amazon VPC nos seguintes tópicos:

- ClassicLink
- Listas de prefixos gerenciados (p. 272)
- Espelhamento de tráfego
- Gateways de trânsito
- VPC endpoints e serviços de VPC endpoint
- Políticas de VPC endpoint
- Emparelhamento de VPC
- AWS Wavelength

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.

Tópicos

- Não tenho autorização para executar uma ação na Amazon VPC (p. 177)
- Não estou autorizado a executar iam:PassRole (p. 177)
- Quero visualizar minhas chaves de acesso (p. 177)
- Sou administrador e desejo permitir que outros usuários tenham acesso à Amazon VPC (p. 178)

- Quero permitir que pessoas fora da minha conta da AWS acessem meus recursos da Amazon VPC (p. 178)

Não tenho autorização para executar uma ação na Amazon VPC

Se o Console de Gerenciamento da AWS informar que você não está autorizado a executar uma ação, entre em contato com o administrador para obter assistência. O administrador é a pessoa que forneceu a você o seu nome de usuário e senha.

O exemplo de erro a seguir ocorre quando o usuário `mateojackson` do IAM tenta usar o console para visualizar detalhes sobre uma sub-rede, mas não tem as permissões `ec2:DescribeSubnets`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:DescribeSubnets on resource: subnet-id
```

Neste caso, Mateo pede ao administrador para atualizar suas políticas para permitir que ele acesse a sub-rede.

Não estou autorizado a executar iam:PassRole

Se você receber uma mensagem de erro informando que você não está autorizado a executar a ação `iam:PassRole`, entre em contato com o administrador para obter assistência. O administrador é a pessoa que forneceu a você o seu nome de usuário e senha. Peça a essa pessoa para atualizar suas políticas a fim de permitir que você transmita uma função à Amazon VPC.

Alguns serviços da AWS permitem que você transmita uma função existente para o serviço, em vez de criar uma função de serviço ou uma função vinculada ao serviço. Para fazer isso, um usuário deve ter permissões para passar a função 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 uma função de serviço. Mary não tem permissões para passar a função para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

Neste caso, Mary pede ao administrador para atualizar suas políticas para permitir que ela execute a ação `iam:PassRole`.

Quero visualizar minhas chaves de acesso

Depois de criar suas chaves de acesso de usuário do IAM, é possível visualizar seu ID da chave de acesso a qualquer momento. No entanto, você não pode visualizar sua chave de acesso secreta novamente. Se você perder sua chave secreta, crie um novo par de chaves de acesso.

As chaves de acesso consistem em duas partes: um ID de chave de acesso (por exemplo, `AKIAIOSFODNN7EXAMPLE`) e uma chave de acesso secreta (por exemplo, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Como um nome de usuário e uma senha, você deve usar o ID da chave de acesso e a chave de acesso secreta em conjunto para autenticar suas solicitações. Gerencie suas chaves de acesso de forma tão segura quanto você gerencia seu nome de usuário e sua senha.

> **Important**
>
> Não forneça as chaves de acesso a terceiros, mesmo que seja para ajudar a encontrar o ID de usuário canônico. Ao fazer isso, você pode dar a alguém acesso permanente à sua conta.

Ao criar um par de chaves de acesso, você é solicitado a guardar o ID da chave de acesso e a chave de acesso secreta em um local seguro. A chave de acesso secreta só está disponível no momento em

que é criada. Se você perder sua chave de acesso secreta, será necessário adicionar novas chaves de acesso para seu usuário do IAM. Você pode ter no máximo duas chaves de acesso. Se você já tiver duas, você deverá excluir um par de chaves para poder criar um novo. Para visualizar as instruções, consulte Gerenciar chaves de acesso no Guia do usuário do IAM.

Sou administrador e desejo permitir que outros usuários tenham acesso à Amazon VPC

Para permitir que outros usuários acessem a Amazon VPC, é necessário criar uma entidade do IAM (usuário ou função) para a pessoa ou a aplicação que precisa do acesso. Eles usarão as credenciais dessa entidade para acessar a AWS. Você deve anexar uma política à entidade que concede a eles as permissões corretas na Amazon VPC.

Para começar a usar imediatamente, consulte Criar os primeiros usuário e grupo delegados do IAM no Guia do usuário do IAM.

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. Você pode especificar quem é confiável para assumir a função. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso a 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 (p. 166).
- Para saber como conceder acesso aos seus recursos em todas as contas da AWS pertencentes a você, consulte Conceder acesso a um usuário do IAM em outra conta da AWS pertencente a você no Guia do usuário do IAM.
- Para saber como conceder acesso aos recursos para contas da AWS de terceiros, consulte Conceder 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 saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Como as funções do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Registro em log e monitoramento para a Amazon VPC

É possível usar as ferramentas de monitoramento automatizadas a seguir para supervisionar componentes na VPC e gerar relatórios quando algo estiver errado:

- 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 Network ACL e grupos de segurança excessivamente restritivos ou permissivos. Para obter mais informações, consulte VPC Flow Logs (p. 310).
- Monitorar gateways NAT: é possível monitorar o gateway NAT usando o CloudWatch que coleta informações do gateway NAT e cria métricas legíveis quase em tempo real. Para obter mais informações, consulte Monitorar gateways NAT usando o Amazon CloudWatch (p. 236).

Resiliência na Amazon Virtual Private Cloud

A infraestrutura global da AWS é criada com base em regiões e zonas de disponibilidade da AWS. As regiões da AWS fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, altas taxas de transferência e redes altamente redundantes. Com as zonas de disponibilidade, você pode projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre regiões e zonas de disponibilidade da AWS, consulte Infraestrutura global da AWS.

Além da infraestrutura global da AWS, a Amazon VPC oferece vários recursos para ajudar a atender às necessidades de resiliência de dados e backup.

- Opções de conectividade de Amazon VPC para Amazon VPC
- Opções de conectividade de rede para Amazon VPC

Validação de conformidade da Amazon Virtual Private Cloud

Auditores externos avaliam a segurança e a conformidade dos serviços da AWS como parte de vários programas de conformidade da AWS, como SOC, PCI, FedRAMP e HIPAA.

Para obter uma lista de serviços da AWS que estão no escopo de programas de conformidade específicos, consulte Serviços da AWS no escopo por programa de conformidade. Para obter informações gerais, consulte Programas de conformidade da AWS.

É possível fazer download de relatórios de auditoria externa usando o AWS Artifact. Para obter mais informações, consulte Fazer download de relatórios no AWS Artifact.

Sua responsabilidade de conformidade ao usar os 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 seguintes recursos para ajudar com a conformidade:

- Guias de referência rápida de conformidade e segurança: esses guias de implantação abordam as considerações de arquitetura e fornecem etapas para implantação de ambientes de linha de base concentrados em conformidade e segurança na AWS.
- Whitepaper Arquitetura para segurança e conformidade com HIPAA: esse whitepaper descreve como as empresas podem usar a AWS para criar aplicações em conformidade com a HIPAA.

  Note

  Nem todos os serviços estão em conformidade com a HIPAA.
- Recursos de conformidade da AWS: essa coleção de manuais e guias pode ser aplicada ao seu setor e local.
- 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: esse serviço da AWS fornece um panorama abrangente do seu estado de segurança dentro da AWS, ajudando você a verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança.
- AWS Audit Manager: esse serviço da AWS ajuda a auditar continuamente o uso da AWS para simplificar a forma como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

Análise de configuração e vulnerabilidade na Amazon Virtual Private Cloud

A configuração e os controles de TI são uma responsabilidade compartilhada da AWS e sua, nosso cliente. Para obter mais informações, consulte o modelo de responsabilidade compartilhada da AWS. Além do modelo de responsabilidade compartilhada, os usuários da VPC devem estar cientes do seguinte:

- É da responsabilidade do cliente corrigir as aplicações de clientes com as dependências relevantes do lado do cliente.
- Os clientes devem considerar testes de penetração para gateways NAT e instâncias do EC2 (consulte https://aws.amazon.com/security/penetration-testing/).

Grupos de segurança para a VPC

Um security group atua como um firewall virtual para sua instância para controlar o tráfego de entrada e saída. Quando você executa uma instância na VPC, é possível atribuir até cinco grupos de segurança à instância. Os grupos de segurança atuam no nível da instância e não no nível da sub-rede. Portanto, cada instância em uma sub-rede em sua VPC pode ser atribuída a um conjunto diferente de grupos de segurança.

Se você executar uma instância usando a API do Amazon EC2 ou uma ferramenta da linha de comando e não especificar um grupo de segurança, a instância será atribuída automaticamente ao grupo de segurança padrão da VPC. Se você executar uma instância usando o console do Amazon EC2, terá a opção de criar um grupo de segurança para a instância.

Para cada security group, adicione regras que controlam o tráfego de entrada para instâncias e um conjunto separado de regras que controlam o tráfego de saída. Esta seção descreve as informações básicas que você precisa saber sobre grupos de segurança para a VPC e suas regras.

Você pode configurar Network ACLs com regras semelhantes às dos grupos de segurança a fim de adicionar uma camada extra de segurança à sua VPC. Para obter mais informações sobre as diferenças entre security groups e Network ACLs, consulte Comparação entre grupos de segurança e network ACLs (p. 159).

Tópicos

Noções básicas do grupo de segurança

Veja a seguir as características básicas dos grupos de segurança da sua VPC:

- Você pode especificar regras de permissão, mas não regras de negação.
- Você pode especificar regras separadas para o tráfego de entrada e de saída.
- As regras do grupo de segurança permitem filtrar o tráfego com base em protocolos e números de porta.
- Os grupos de segurança são do tipo com estado: se você enviar uma solicitação da instância, o tráfego da resposta dessa solicitação terá permissão para fluir, independentemente das regras de

entrada do grupo de segurança. As respostas ao tráfego permitido de entrada são permitidas para fluir, independentemente das regras de saída.

> **Note**
>
> Alguns tipos de tráfego são rastreados de forma diferente de outros. Para obter mais informações, consulte Rastreamento de conexões no Guia do usuário do Amazon EC2 para instâncias do Linux.

- Quando você cria um grupo de segurança, ele não possui regras de entrada. Portanto, nenhum tráfego de entrada originário de outro host para a instância será permitido até que você adicione regras de entrada ao security group.
- Por padrão, um security group inclui uma regra de saída que permite todo o tráfego de saída. Você pode remover a regra e adicionar regras de saída que permitem somente tráfego de saída específico. Se o security group não tiver nenhuma regra de saída, nenhum tráfego de saída originário da instância será permitido.
- 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 obter mais informações, consulte Cotas da Amazon VPC (p. 345).
- As instâncias associadas a um grupo de segurança não podem se comunicar entre elas, a menos que você adicione regras que permitam a comunicação (exceção: o grupo de segurança padrão já tem essas regras).
- Os security groups estão associados a interfaces de rede. Depois de iniciar uma instância, você pode alterar os grupos de segurança associados à instância, o que altera os grupos de segurança associados à interface de rede principal (eth0). Também é possível especificar ou alterar os grupos de segurança associados a qualquer outra interface de rede. Por padrão, quando você cria uma interface de rede, ela é associada ao grupo de segurança padrão da VPC, a menos que você especifique outro grupo de segurança. Para obter mais informações sobre interfaces de rede, consulte Interfaces de rede elástica.
- Ao criar um security group, você deve fornecer um nome e uma descrição. As seguintes regras se aplicam:
  - 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 contém espaços finais, removemos os espaços ao salvar o nome. Por exemplo, se você inserir "Grupo de segurança de teste " para o nome, nós o armazenamos como "Grupo de segurança de teste".
  - Um nome de grupo de segurança não pode começar com `sg-`, pois esse prefixo indica um grupo de segurança padrão.
  - O nome do grupo de segurança deve ser exclusivo dentro da VPC.
- Um grupo de segurança só poderá ser usado na VPC especificada quando você criá-lo.

Grupo de segurança padrão para a VPC

Sua VPC vem automaticamente com um grupo de segurança padrão. Se você não especificar um grupo de segurança diferente ao executar a instância, associaremos o grupo de segurança padrão à instância.

> **Note**
>
> Se você executar uma instância no console do Amazon EC2, o assistente de execução de instância definirá automaticamente um grupo de segurança "launch-wizard-*xx*", que pode ser associado à instância em vez do grupo de segurança padrão.

A tabela a seguir descreve as regras padrão para um security group padrão.

Inbound			
Source	Protocol	Port range	Description
O ID do security group (sg-xxxxxxxx)	Tudo	Todos	Permitir tráfego de entrada de interfaces de rede (e suas instâncias associadas) atribuídas ao mesmo grupo de segurança.
Outbound			
Destination	Protocol	Port range	Description
0.0.0.0/0	Tudo	Tudo	Permitir todo o tráfego IPv4 de saída.
::/0	Tudo	Tudo	Permitir todo o tráfego IPv6 de saída. Esta regra é adicionada por padrão se você criar uma VPC com um bloco CIDR IPv6 ou se você associar um bloco CIDR IPv6 a sua VPC existente.

Você pode alterar as regras do security group padrão.

Você não pode excluir um security group padrão. Se você tentar excluir o grupo de segurança padrão, o seguinte erro será exibido: `Client.CannotDelete: the specified group: "sg-51530134" name: "default" cannot be deleted by a user`.

> **Note**
>
> Se você modificou as regras de saída do seu security group, não adicionaremos automaticamente uma regra de saída para o tráfego IPv6 quando você associar um bloco IPv6 a sua VPC.

Regras de grupos de segurança

Você pode adicionar ou remover regras de um security group (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 um intervalo CIDR específico ou a outro security group em sua VPC ou em um par da VPC (requer uma conexão de emparelhamento de VPC).

A seguir estão as partes básicas de uma regra de security group em uma VPC:

- (Regras de entrada somente) A origem do tráfego e a porta de destino ou o intervalo da porta. A origem pode ser outro grupo de segurança, um bloco CIDR IPv4 ou IPv6, um único endereço IPv4 ou IPv6 ou um ID de lista de prefixos.
- (Regras de saída somente) O destino do tráfego e a porta de destino ou o intervalo da porta. O destino pode ser outro grupo de segurança, um bloco CIDR IPv4 ou IPv6, um único endereço IPv4 ou IPv6 ou um ID de lista de prefixos.
- Qualquer protocolo que tem um número de protocolo padrão (para obter uma lista, consulte Números de protocolo). Se você especificar o ICMP como protocolo, poderá especificar qualquer ou todos os tipos e códigos ICMP.

- Uma descrição opcional para a regra do security group para ajudar a identificá-lo posteriormente. Uma descrição pode ser até 255 caracteres de comprimento. Os caracteres permitidos são a-z, A-Z, 0-9, espaços e ._-:/()#,@[]+=;{}!$*.
- Se você adicionar uma regra de grupo de segurança usando a CLI da AWS, o console ou a API, definiremos automaticamente o bloco CIDR de origem ou de destino como a forma canônica. Por exemplo, se você especificar 100.68.0.18/18 para o bloco CIDR, criaremos uma regra com um bloco CIDR de 100.68.0.0/18.

Quando você especifica um bloco CIDR como a origem de uma regra, o tráfego dos endereços especificados para o protocolo e a porta especificados é habilitado.

Quando você especifica um grupo de segurança como a origem de uma regra, o tráfego das interfaces de rede associadas ao grupo de segurança de origem é permitido para o protocolo e a porta especificados. O tráfego de entrada é permitido com base nos endereços IP privados das interfaces de rede associadas ao grupo de segurança de origem (e não aos endereços IP público ou IP elástico). Adicionar um security group como origem não adiciona regras nesse security group de origem. Para ver um exemplo, consulte Grupo de segurança padrão para a VPC (p. 181).

Se você especificar um único endereço IPv4, especifique-o usando o comprimento de prefixo /32. Se você especificar um único endereço IPv6, especifique-o usando o comprimento de prefixo /128.

Alguns sistemas para configurar firewalls permitem que você filtre nas portas de origem. Os grupos de segurança permitem que você filtre apenas nas portas de destino.

Quando você adiciona ou remove regras, elas são aplicadas automaticamente a todas as instâncias associadas ao security group.

O tipo de regras adicionadas pode depender da finalidade do grupo de segurança. A tabela a seguir descreve regras de exemplo para um grupo de segurança associado a servidores da web. Os servidores da web podem receber tráfego HTTP e HTTPS de todos os endereços IPv4 e IPv6 e enviar tráfego SQL ou MySQL para um servidor de banco de dados.

Inbound			
Source	Protocol	Port range	Description
0.0.0.0/0	TCP	80	Permitir acesso HTTP de entrada de todos os endereços IPv4
::/0	TCP	80	Permitir acesso HTTP de entrada de todos os endereços IPv6
0.0.0.0/0	TCP	443	Permitir acesso HTTPS de entrada de todos os endereços IPv4
::/0	TCP	443	Permitir acesso HTTPS de entrada de todos os endereços IPv6
O alcance do endereço IPv4 público da sua rede	TCP	22	Permitir acesso SSH de entrada para instâncias Linux a partir de endereços IP IPv4 na sua rede (pelo gateway da Internet)

O alcance do endereço IPv4 público da sua rede	TCP	3389	Permitir acesso de entrada ao RDP para instâncias Windows a partir de endereços IP IPv4 na sua rede (pelo gateway da Internet)

Outbound

Destination	Protocol	Port range	Description
O ID do grupo de segurança dos servidores de banco de dados do Microsoft SQL Server	TCP	1433	Permitir o acesso do Microsoft SQL Server de saída a instâncias no security group especificado
O ID do security group para seus servidores de banco de dados MySQL	TCP	3306	Permitir acesso MySQL de saída a instâncias no security group especificado

Um servidor de banco de dados precisaria de outro conjunto de regras. Por exemplo, em vez de tráfego HTTP e HTTPS de entrada, é possível adicionar uma regra que permita acesso MySQL ou Microsoft SQL Server de entrada. Para obter um exemplo de regras de security group para servidores Web e servidores de banco de dados, consulte Segurança (p. 58). Para obter mais informações sobre grupos de segurança para instâncias de banco de dados do RDS, consulte Controlar acesso com grupos de segurança no Guia do usuário do Amazon RDS.

Para obter exemplos de regras de grupos de segurança para tipos de acesso específicos, consulte Referência de regras de grupos de segurança no Guia do usuário do Amazon EC2 para instâncias do Linux.

Regras de grupo de segurança obsoletas

Se a VPC tiver uma conexão de emparelhamento de VPC com outra VPC, uma regra do security group pode fazer referência a outro security group no par da VPC. Isso permite que as instâncias associadas ao grupo de segurança referenciado e aquelas associadas ao grupo de segurança de referência se comuniquem entre elas.

Se o proprietário do par da VPC excluir o security group especificado ou se você ou o proprietário do par da VPC excluir a conexão de emparelhamento de VPC, a regra do security group será marcada como `stale`. Você pode excluir regras de security group obsoletas, como faria com qualquer outra regra do security group.

Para obter mais informações, consulte Trabalhar com grupos de segurança obsoletos no Guia de emparelhamento da Amazon VPC.

Diferenças entre grupos de segurança para EC2-Classic e EC2-VPC

Você não pode usar os grupos de segurança criados no EC2-Classic com instâncias em sua VPC. É necessário criar grupos de segurança específicos para as instâncias da VPC. As regras criadas para o grupo de segurança de uma VPC não podem fazer referência a um grupo de segurança do EC2-Classic e vice-versa. Para obter mais informações sobre as diferenças entre os grupos de segurança a serem

usados com o EC2-Classic e aqueles a serem usados com uma VPC, consulte Diferenças entre o EC2-Classic e uma VPC no Guia do usuário do Amazon EC2 para instâncias do Linux.

Trabalhar com grupos de segurança

As tarefas a seguir mostram como utilizar os grupos de segurança por meio do console da Amazon VPC.

Para obter exemplos de políticas do IAM para trabalhar com grupos de segurança, consulte Gerenciar grupos de segurança (p. 174).

Tarefas

Modificar o grupo de segurança padrão

Sua VPC é fornecida com um grupo de segurança padrão (p. 181). Você não pode excluir este grupo. No entanto, você pode alterar as regras do grupo. O procedimento é o mesmo da modificação de qualquer outro security group. Para obter mais informações, consulte Adicionar, remover e atualizar regras (p. 186).

Criar um grupo de segurança

Embora você possa usar o security group padrão para suas instâncias, é possível criar seus próprios grupos para refletir as diferentes funções que as instâncias desempenham no seu sistema.

O procedimento a seguir cria um grupo de segurança sem regras de entrada e a regra de saída padrão.

Para criar um security group 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 security group (Criar grupo de segurança).
4. Digite um nome para o grupo de segurança (por exemplo, `my-security-group`) e forneça uma descrição.
5. Em VPC, selecione o ID da VPC.
6. (Opcional) Adicione ou remova uma tag.

   [Adicionar uma tag] Escolha Adicionar nova tag e faça o seguinte:

   - Em Key (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 Create (Criar).

Para criar um security group usando a linha de comando

- create-security-group (CLI da AWS)

- New-EC2SecurityGroup (AWS Tools for Windows PowerShell)

Para descrever um ou mais security groups usando a linha de comando

- describe-security-groups (CLI da AWS)
- Get-EC2SecurityGroup (AWS Tools for Windows PowerShell)

Por padrão, novos grupos de segurança começam com apenas uma regra de saída que permite que todo o tráfego deixe as instâncias. Você deve adicionar regras para permitir qualquer tráfego de entrada ou para restringir o tráfego de saída.

Adicionar, remover e atualizar regras

Quando você adicionar ou remover regras, quaisquer instâncias já atribuídas ao security group estarão sujeitas à alteração.

Se você tiver uma conexão de emparelhamento de VPC, você pode fazer referência a grupos de segurança de par da VPC como origem ou destino nas regras do seu security group. Para obter mais informações, consulte Atualização das regras do grupo de segurança para referenciar os grupos de segurança na VPC emparelhada em Guia de emparelhamento da Amazon VPC.

Para adicionar uma regra 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 e especifique a origem (regras de entrada) ou o destino (regras de saída). Por exemplo, para um servidor Web público, selecione HTTP ou HTTPS e especifique um valor para a Source como `0.0.0.0/0`.

   Se você usar `0.0.0.0/0`, permitirá que todos os endereços IPv4 acessem sua instância usando HTTP ou HTTPS. Para restringir o acesso, insira um endereço IP específico ou um intervalo de endereços.
6. Você também pode permitir a comunicação entre todas as instâncias associadas a esse grupo de segurança. Crie uma regra de entrada com as seguintes opções:

   - Type (Tipo): All Traffic (Todo o tráfego)
   - Source (Origem): insira o ID do grupo de segurança.
7. Selecione Save rules (Salvar regras).

Para excluir uma regra 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 Delete (Excluir) para a regra que você deseja excluir.
6. Selecione Save rules (Salvar regras).

Quando você modifica o protocolo, o intervalo de portas ou a origem ou o destino de um security group existente usando o console, o console exclui a regra existente e adiciona uma nova para você.

Para atualizar uma regra 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. Modifique entrada de regra conforme necessário.
6. Selecione Save rules (Salvar regras).

Se você estiver atualizando o protocolo, o intervalo de portas, a origem ou o destino de uma regra existente usando a API do Amazon EC2 ou uma ferramenta de linha de comando, não será possível modificar a regra. Em vez disso, você deve excluir a regra existente e adicionar uma regra nova. Para atualizar apenas a descrição da regra, você pode usar os comandos update-security-group-rule-descriptions-ingress e update-security-group-rule-descriptions-egress.

Para adicionar uma regra a um security group usando a linha de comando

- authorize-security-group-ingress e authorize-security-group-egress (CLI da AWS)
- Grant-EC2SecurityGroupIngress e Grant-EC2SecurityGroupEgress (AWS Tools for Windows PowerShell)

Para excluir uma regra de um security group usando a linha de comando

- revoke-security-group-ingress e revoke-security-group-egress(CLI da AWS)
- Revoke-EC2SecurityGroupIngress e Revoke-EC2SecurityGroupEgress (AWS Tools for Windows PowerShell)

Para atualizar a descrição da regra de um security group usando a linha de comando

- update-security-group-rule-descriptions-ingress e update-security-group-rule-descriptions-egress (CLI da AWS)
- Update-EC2SecurityGroupRuleIngressDescription e Update-EC2SecurityGroupRuleEgressDescription (AWS Tools for Windows PowerShell)

Alterar grupos de segurança de uma Instância

Após iniciar uma instância em uma VPC, você pode alterar os grupos de segurança associados à instância. Você pode alterar os grupos de segurança para uma instância quando a instância está no estado `running` ou `stopped`.

> **Note**
>
> Este procedimento altera os grupos de segurança associados à interface de rede primária (eth0) da instância. Para alterar os grupos de segurança de outras interfaces de rede, consulte Alterar o grupo de segurança.

Para alterar os grupos de segurança de uma instância usando o console

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

3. Marque a caixa de seleção da instância. A guia Security (Segurança) lista os grupos de segurança associados à instância.
4. Para alterar os grupos de segurança associados à instância, escolha Actions (Ações), Security (Segurança) , Change security groups (Alterar grupos de segurança) .
5. Em Associated security groups, selecione um grupo de segurança na lista e escolha Add security group.

   Para remover um grupo de segurança já associado, escolha Remove (Remover) para esse grupo de segurança.
6. Escolha Save (Salvar).

Para alterar os grupos de segurança de uma instância usando a linha de comando

- modify-instance-attribute (CLI da AWS)
- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Excluir um grupo de segurança

Você pode excluir um security group somente se não houver instâncias atribuídas (executadas ou interrompidas). Você pode atribuir as instâncias a outro security group antes de excluir o security group (consulte Alterar grupos de segurança de uma Instância (p. 187)). Você não pode excluir um security group padrão.

Se você estiver usando o console, pode excluir mais de um security group por vez. Se você estiver usando a linha de comando ou a API, pode excluir apenas um security group por vez.

Para excluir um security group 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 um ou mais grupos de segurança e escolha Ações do security group, Excluir security group.
4. Na caixa de diálogo Delete Security Group, selecione Sim, excluir.

Para excluir um security group usando a linha de comando

- delete-security-group (CLI da AWS)
- Remove-EC2SecurityGroup (AWS Tools for Windows PowerShell)

Excluir o grupo de segurança padrão de 15-07-2009

Qualquer VPC criada usando uma versão da API depois de 2011-01-01 tem o security group `2009-07-15-default`. Este security group existe, além do security group `default` regular que vem com cada VPC. Não é possível associar um gateway da Internet a uma VPC que tenha o grupo de segurança `2009-07-15-default`. Portanto, você precisa excluir esse grupo de segurança para poder associar um gateway da Internet à VPC.

> **Note**
>
> Se você atribuiu este security group a quaisquer instâncias, você deve atribuir essas instâncias a um security group diferente antes de excluir o security group.

Para excluir o security group **`2009-07-15-default`**

1. Certifique-se de que este security group não foi atribuído a nenhuma instância.

a. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
b. No painel de navegação, selecione Network Interfaces.
c. Selecione a interface de rede para a instância da lista e selecione Change Security Groups, Actions.
d. Na caixa de diálogo Change Security Groups, selecione um novo security group da lista e selecione Save.

   Ao alterar o security group de uma instância, você pode selecionar vários grupos da lista. Os grupos de segurança que você seleciona substituem os security groups atuais da instância.
e. Repita as etapas do procedimento para cada instância.

2. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
3. No painel de navegação, selecione Grupos de segurança.
4. Escolha o grupo de segurança `2009-07-15-default` e, em seguida, Security Group Actions, Delete Security Group.
5. Na caixa de diálogo Delete Security Group, selecione Sim, excluir.

Gerenciar centralmente os grupos de segurança da VPC usando o AWS Firewall Manager

O AWS Firewall Manager simplifica as tarefas de administração e manutenção dos grupos de segurança na VPC em várias contas e recursos. Com o Firewall Manager, é possível configurar e auditar os grupos de segurança para a organização a partir de uma única conta de administrador central. O Firewall Manager aplica automaticamente as regras e as proteções em todas as contas e recursos, mesmo na adição de novos recursos. O Firewall Manager é particularmente útil quando você deseja proteger toda a sua organização ou se você adiciona frequentemente novos recursos que deseja proteger de uma conta de administrador central.

É possível usar o Firewall Manager para gerenciar centralmente os grupos de segurança das seguintes maneiras:

- Configurar grupos de segurança de base comum em toda a organização: você pode usar uma política comum de grupo de segurança para fornecer uma associação de grupos de segurança, controlada centralmente, a contas e recursos em toda a organização. Você especifica onde e como aplicar a política em sua organização.
- Auditoria de grupos de segurança existentes na organização: você pode usar uma política de grupo de segurança de auditoria para verificar as regras existentes em uso nos grupos de segurança da organização. É possível avaliar a política para auditar todas as contas, contas específicas ou recursos marcados com tags na organização. O Firewall Manager detecta automaticamente novas contas e recursos e as auditora. Você pode criar regras de auditoria para definir proteções nas regras do grupo de segurança que devem ser permitidas ou não na sua organização e para verificar grupos de segurança não usados ou redundantes.
- Obter relatórios sobre recursos incompatíveis e corrigi-los: você pode obter relatórios e alertas para recursos incompatíveis com as políticas de base e auditoria. Também é possível definir fluxos de trabalho de autorremediação para corrigir quaisquer recursos incompatíveis detectados pelo Firewall Manager.

Para saber mais sobre como usar o Firewall Manager para gerenciar os grupos de segurança, consulte os tópicos a seguir no Guia do desenvolvedor do AWS WAF:

- Pré-requisitos do AWS Firewall Manager
- Conceitos básicos das políticas de grupo de segurança da Amazon VPC do AWS Firewall Manager

- Como funcionam as políticas de grupo de segurança no AWS Firewall Manager
- Casos de uso da política de grupo de segurança

Network ACLs

Uma lista de controle de acesso (ACL) à rede é uma camada de segurança opcional para sua VPC que funciona como firewall para controlar o tráfego de entrada e saída de uma ou mais sub-redes. Você pode configurar Network ACLs com regras semelhantes às dos grupos de segurança a fim de adicionar uma camada extra de segurança à sua VPC. Para obter mais informações sobre as diferenças entre security groups e Network ACLs, consulte Comparação entre grupos de segurança e network ACLs (p. 159).

Tópicos

Noções básicas de network ACL

Encontram-se a seguir noções essenciais sobre as Network ACLs:

- Sua VPC já vem com uma Network ACL padrão modificável. Por padrão, ela permite todos os tráfegos de IPv4 de entrada e saída e, se aplicável, o tráfego IPv6.
- Você pode criar uma Network ACL personalizada e associá-la a uma sub-rede. Por padrão, enquanto você não adicionar regras, toda Network ACL personalizada negará todo e qualquer tráfego de entrada e saída.
- Toda sub-rede em sua VPC deve ser associada com uma Network ACL. Se você não associar explicitamente uma sub-rede com uma Network ACL, as sub-redes serão associadas automaticamente com a Network ACL padrão.
- É possível associar uma network ACL a várias sub-redes. No entanto, uma sub-rede pode ser associada a apenas uma network ACL por vez. Quando uma Network ACL é associada a uma sub-rede, a associação anterior é removida.
- Uma network ACL contém uma lista numerada de regras. Avaliamos as regras em ordem, começando com a regra de menor número, para determinar se o tráfego pode entrar ou sair de qualquer sub-rede associada à network ACL. O número mais alto que é possível usar para uma regra é 32766. Para começar, é recomendável criar regras em incrementos (por exemplo, incrementos de 10 ou 100), para que posteriormente você possa inserir novas regras onde precisar.
- Uma Network ACL tem regras de entrada e saída distintas e cada uma pode permitir ou negar tráfego.
- As ACLs de rede são stateless, o que significa que as respostas para o tráfego de entrada permitido estão sujeitas às regras para o tráfego de saída (e vice-versa).

Há cotas (limites) para o número de network ACLs por VPC e o número de regras por network ACL. Para obter mais informações, consulte Cotas da Amazon VPC (p. 345).

Regras de network ACL

Você pode adicionar ou remover regras de Network ACL padrão ou criar outras Network ACLs para sua VPC. Ao adicionar ou remover regras de uma network ACL, as alterações são automaticamente aplicadas às sub-redes às quais ela está associada.

Encontram-se a seguir as partes de uma regras de Network ACL:

- 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.
- 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.
- Fonte. [Somente regras de entrada] A origem do tráfego (intervalo CIDR).
- Destino. [Somente regras de saída] O destino do tráfego (intervalo CIDR).
- Permissão/Negação. Se permite ou nega o tráfego especificado.

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`.

Network ACL padrão

A network ACL padrão é configurada para permitir todo o tráfego de entrada e saída das sub-redes com as quais está associada. Além disso, toda Network ACL contém uma regra cujo número é um asterisco. Essa regra garante que, se um pacote não corresponder a nenhuma das outras regras numeradas, o acesso seja negado. Não é possível modificar nem remover essa regra.

Encontra-se a seguir um exemplo de Network ACL padrão para uma VPC compatível somente com IPv4.

Entrada					
Regra nº	Tipo	Protocolo	Intervalo de portas	Origem	Permissão/ Negação
100	Todo tráfego IPv4	Tudo	Todos	0.0.0.0/0	PERMISSÃO
*	Todo tráfego IPv4	Tudo	Todos	0.0.0.0/0	NEGAÇÃO
Saída					
Regra nº	Tipo	Protocolo	Intervalo de portas	Destino	Permissão/ Negação
100	Todo tráfego IPv4	Tudo	Todos	0.0.0.0/0	PERMISSÃO

*	Todo tráfego IPv4	Tudo	Todos	0.0.0.0/0	NEGAÇÃO

Se você criar uma VPC com um bloco CIDR IPv6 ou se associar um bloco CIDR IPv6 à VPC existente, adicionaremos automaticamente as regras que permitem todo tráfego IPv6 de entrada e saída em sua sub-rede. Além disso, adicionamos regras cujos números são um asterisco que garante que um pacote tenha acesso negado se não corresponder a nenhuma outra regra numerada. Não é possível modificar nem remover essas regras. Encontra-se a seguir um exemplo de Network ACL padrão para uma VPC compatível com IPv4 e IPv6.

> **Note**
>
> Se tiver modificado as regras de entrada de sua network ACL padrão, não adicionaremos automaticamente uma regra de permissão para tráfego IPv6 de entrada quando você associar um bloco IPv6 à sua VPC. Do mesmo modo, se tiver modificado as regras de saída, não adicionaremos automaticamente uma regra de permissão para tráfego IPv6 de saída.

Entrada					
Regra nº	Tipo	Protocolo	Intervalo de portas	Origem	Permissão/ Negação
100	Todo tráfego IPv4	Tudo	Todos	0.0.0.0/0	PERMISSÃO
101	Todo tráfego IPv6	Tudo	Tudo	::/0	PERMISSÃO
*	Todo o tráfego	Tudo	Todos	0.0.0.0/0	NEGAÇÃO
*	Todo tráfego IPv6	Tudo	Tudo	::/0	NEGAÇÃO
Saída					
Regra nº	Tipo	Protocolo	Intervalo de portas	Destino	Permissão/ Negação
100	Todo o tráfego	Tudo	Todos	0.0.0.0/0	PERMISSÃO
101	Todo tráfego IPv6	Tudo	Tudo	::/0	PERMISSÃO
*	Todo o tráfego	Tudo	Todos	0.0.0.0/0	NEGAÇÃO
*	Todo tráfego IPv6	Tudo	Tudo	::/0	NEGAÇÃO

Network ACL personalizada

A tabela a seguir mostra um exemplo de uma Network ACL padrão para uma VPC compatível somente com IPv4. Isso inclui regras que permitem tráfego HTTP e HTTPS de entrada (regras de entrada 100 e 110). Existe uma regra de saída correspondente que permite respostas ao tráfego de entrada (regra de saída 140, que abrange portas efêmeras 32768-65535). Para obter mais informações sobre como selecionar o intervalo de portas efêmero apropriado, consulte Portas efêmeras (p. 202).

A Network ACL tem também regras que permitem tráfego SSH e RDP para a sub-rede. A regra de saída 120 permite a saída de respostas da sub-rede.

A Network ACL tem regras de saída (100 e 110) que permitem tráfego HTTP e HTTPS de saída fora da sub-rede. Existe uma regra de entrada correspondente que permite respostas a esse tráfego de saída (regra de entrada 140, que abrange portas efêmeras 32768-65535).

Note

Além disso, toda Network ACL contém uma regra padrão cujo número é um asterisco. Essa regra garante que, se um pacote não corresponder a nenhuma das outras regras, o acesso seja negado. Não é possível modificar nem remover essa regra.

Entrada						
Regra nº	Tipo	Protocolo	Intervalo de portas	Origem	Permissão/ Negação	Comentários
100	HTTP	TCP	80	0.0.0.0/0	PERMISSÃO	Permite tráfego HTTP de entrada de qualquer endereço IPv4.
110	HTTPS	TCP	443	0.0.0.0/0	PERMISSÃO	Permite tráfego HTTPS de entrada de qualquer endereço IPv4.
120	SSH	TCP	22	192.0.2.0/24	PERMISSÃO	Permite tráfego SSH de entrada de um intervalo de endereços IPv4 públicos de sua rede doméstica (no gateway da Internet).
130	RDP	TCP	3389	192.0.2.0/24	PERMISSÃO	Permite tráfego RDP de entrada de um intervalo de endereços IPv4 públicos de sua rede doméstica para servidores web (no

						gateway da Internet).
140	TCP personalizado	TCP	32768-65535	0.0.0.0/0	PERMISSÃO	Permite tráfego IPv4 de retorno de entrada da Internet (isto é, para solicitações originadas na sub-rede). O intervalo é apenas de exemplo. Para obter mais informações sobre como selecionar o intervalo de portas efêmero apropriado, consulte Portas efêmeras (p. 202).
*	Todo o tráfego	Tudo	Todos	0.0.0.0/0	NEGAÇÃO	Nega todos os tráfegos IPv4 de entrada ainda não controlados por uma regra precedente (não modificável).
Saída						
Regra nº	Tipo	Protocolo	Intervalo de portas	Destino	Permissão/ Negação	Comentários
100	HTTP	TCP	80	0.0.0.0/0	PERMISSÃO	Permite tráfego HTTP IPv4 de saída da sub-rede para a Internet.

110	HTTPS	TCP	443	0.0.0.0/0	PERMISSÃO	Permite tráfego HTTPS IPv4 de saída da sub-rede para a Internet.
120	SSH	TCP	22	192.0.2.0/24	PERMISSÃO	Permite tráfego SSH de saída de um intervalo de endereços IPv4 públicos de sua rede doméstica (no gateway da Internet).
140	TCP personalizado	TCP	32768-65535	0.0.0.0/0	PERMISSÃO	Permite respostas IPv4 de saída a clientes na Internet (por exemplo, fornece páginas web a pessoas que visitam os servidores web na sub-rede). O intervalo é apenas de exemplo. Para obter mais informações sobre como selecionar o intervalo de portas efêmero apropriado, consulte Portas efêmeras (p. 202).

*	Todo o tráfego	Tudo	Todos	0.0.0.0/0	NEGAÇÃO	Nega todos os tráfegos IPv4 de saída ainda não controlados por uma regra precedente (não modificável).

Quando um pacote chega à sub-rede, nós o avaliamos com base em regras de entrada da ACL com a qual a sub-rede está associada (do topo da lista de regras para baixo). Veja como a avaliação ocorre quando o pacote é destinado para a porta HTTPS (443). O pacote não corresponde à primeira regra avaliada (regra 100). Ele corresponde à segunda regra (110), que permite que o pacote entre na sub-rede. Se o pacote tiver sido destinado para a porta 139 (NetBIOS), ele não será mais compatível com nenhuma das regras, e a regra * acabará negando o pacote.

É recomendável adicionar uma regra de negação em uma situação em que você precisa verdadeiramente abrir um amplo intervalo de portas, mas existem determinadas portas nesse intervalo às quais deseja negar acesso. Não se esqueça de inserir a regra de negação na tabela antes da regra que permite o tráfego a um amplo intervalo de portas.

Adicione regras de permissão dependendo do seu caso de uso. Por exemplo, é possível adicionar uma regra que permita acesso TCP e UDP de saída na porta 53 para resolução DNS. Para cada regra adicionada, certifique-se de que haja uma regra de entrada ou de saída que permita o tráfego de resposta.

A tabela a seguir mostra o mesmo exemplo de uma Network ACL personalizada para uma VPC que tem um bloco CIDR IPv6 associado. Essa Network ACL contém regras para todo tráfego HTTP e HTTPS IPv6. Nesse caso, novas regras foram inseridas entre as regras existentes para o tráfego IPv4. Também é possível adicionar as regras como regras de número mais alto após as regras IPv4. Os tráfegos IPv4 e IPv6 são diferentes; portanto, nenhuma das regras para tráfego IPv4 se aplica ao tráfego IPv6.

Entrada						
Regra nº	Tipo	Protocolo	Intervalo de portas	Origem	Permissão/ Negação	Comentários
100	HTTP	TCP	80	0.0.0.0/0	PERMISSÃO	Permite tráfego HTTP de entrada de qualquer endereço IPv4.
105	HTTP	TCP	80	::/0	PERMISSÃO	Permite tráfego HTTP de entrada de qualquer endereço IPv6.
110	HTTPS	TCP	443	0.0.0.0/0	PERMISSÃO	Permite tráfego

						HTTPS de entrada de qualquer endereço IPv4.
115	HTTPS	TCP	443	::/0	PERMISSÃO	Permite tráfego HTTPS de entrada de qualquer endereço IPv6.
120	SSH	TCP	22	192.0.2.0/24	PERMISSÃO	Permite tráfego SSH de entrada de um intervalo de endereços IPv4 públicos de sua rede doméstica (no gateway da Internet).
130	RDP	TCP	3389	192.0.2.0/24	PERMISSÃO	Permite tráfego RDP de entrada de um intervalo de endereços IPv4 públicos de sua rede doméstica para servidores web (no gateway da Internet).

140	TCP personalizado	TCP	32768-65535	0.0.0.0/0	PERMISSÃO	Permite tráfego IPv4 de retorno de entrada da Internet (isto é, para solicitações originadas na sub-rede). O intervalo é apenas de exemplo. Para obter mais informações sobre como selecionar o intervalo de portas efêmero apropriado, consulte Portas efêmeras (p. 202).
145	TCP personalizado	TCP	32768-65535	::/0	PERMISSÃO	Permite tráfego IPv6 de retorno de entrada da Internet (isto é, para solicitações originadas na sub-rede). O intervalo é apenas de exemplo. Para obter mais informações sobre como selecionar o intervalo de portas efêmero apropriado, consulte Portas efêmeras (p. 202).

*	Todo o tráfego	Tudo	Todos	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).

Saída

Regra nº	Tipo	Protocolo	Intervalo de portas	Destino	Permissão/ Negação	Comentários
100	HTTP	TCP	80	0.0.0.0/0	PERMISSÃO	Permite tráfego HTTP IPv4 de saída da sub-rede para a Internet.
105	HTTP	TCP	80	::/0	PERMISSÃO	Permite tráfego HTTP IPv6 de saída da sub-rede para a Internet.
110	HTTPS	TCP	443	0.0.0.0/0	PERMISSÃO	Permite tráfego HTTPS IPv4 de saída da sub-rede para a Internet.

115	HTTPS	TCP	443	::/0	PERMISSÃO	Permite tráfego HTTPS IPv6 de saída da sub-rede para a Internet.
140	TCP personalizado	TCP	32768-65535	0.0.0.0/0	PERMISSÃO	Permite respostas IPv4 de saída a clientes na Internet (por exemplo, fornece páginas web a pessoas que visitam os servidores web na sub-rede). O intervalo é apenas de exemplo. Para obter mais informações sobre como selecionar o intervalo de portas efêmero apropriado, consulte Portas efêmeras (p. 202).

145	TCP personalizado	TCP	32768-65535	::/0	PERMISSÃO	Permite respostas IPv6 de saída a clientes na Internet (por exemplo, fornece páginas da web a pessoas que visitam os servidores da web na sub-rede). O intervalo é apenas de exemplo. Para obter mais informações sobre como selecionar o intervalo de portas efêmero apropriado, consulte Portas efêmeras (p. 202).
*	Todo o tráfego	Tudo	Todos	0.0.0.0/0	NEGAÇÃO	Nega todos os tráfegos IPv4 de saída ainda não controlados por uma regra precedente (não modificável).
*	Todo o tráfego	Tudo	Tudo	::/0	NEGAÇÃO	Nega todos os tráfegos IPv6 de saída ainda não controlados por uma regra precedente (não modificável).

Para obter mais exemplos, consulte Regras recomendadas para cenários de assistente de VPC (p. 210).

Network ACLs personalizadas e outros serviços da AWS

Se você criar uma Network ACL, esteja ciente de como ela pode afetar os recursos criados por meio de outros serviços da AWS.

Com o Elastic Load Balancing, se a sub-rede das instâncias de back-end tiver uma network ACL 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 de network ACL recomendadas para os balanceadores de carga e as instâncias de back-end, consulte Network ACLs para balanceadores de carga em uma VPC no Guia do usuário de Classic Load Balancers.

Portas efêmeras

A Network ACL de exemplo na seção precedente usa o intervalo de portas efêmero 32768-65535. Entretanto, é recomendável usar um intervalo diferente para suas Network ACLs 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 as portas 1024-65535.

Por exemplo, se uma solicitação chegar ao servidor da web em sua VPC de um cliente Windows 10 na Internet, sua network ACL precisará de uma regra de saída para permitir o tráfego destinado às portas 49152 a 65535.

Se uma instância na VPC for o cliente que está iniciando uma solicitação, a Network ACL precisará de uma regra de entrada para permitir o tráfego destinado para as portas efêmeras específicas ao tipo de instância (Amazon Linux, Windows Server 2008 etc.).

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.

Path MTU Discovery

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 IPv4, se um host enviar um pacote que seja maior que a MTU do host de recebimento ou que seja maior que a MTU de um dispositivo ao longo do caminho, o host ou dispositivo de recebimento soltará

o pacote e retornará a seguinte mensagem ICMP: `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` (Tipo 3, Código 4). Isto 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 fragmentação na rede. Se um host enviar um pacote que seja maior que a MTU do host de recebimento ou que seja maior que a MTU de um dispositivo ao longo do caminho, o host ou dispositivo de recebimento soltará o pacote e retornará a seguinte mensagem ICMP: `ICMPv6 Packet Too Big (PTB)` (Tipo 2). Isto 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 comunicarem com pares pela Internet, será necessário adicionar a regra de Network ACL 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 de rede (MTU) para a instância do EC2 no Guia do usuário do Amazon EC2 para instâncias do Linux.

Trabalhar com network ACLs

As tarefas a seguir mostram como utilizar Network ACLs por meio do console da Amazon VPC.

Tarefas

- Determinar associações a network ACLs (p. 203)
- Criar uma network ACL (p. 204)
- Adicionar e excluir regras (p. 204)
- Associar uma sub-rede a uma network ACL (p. 205)
- Desassociar uma network ACL de uma sub-rede (p. 205)
- Alterar a network ACL de uma sub-rede (p. 205)
- Excluir uma network ACL (p. 206)
- Visão geral da API e dos comandos (p. 206)

Determinar associações a network ACLs

É possível usar o console da Amazon VPC para determinar qual Network ACL está associada a uma sub-rede. Como as network ACLs podem ser associadas a uma ou mais sub-redes, também é possível determinar as sub-redes que estão associadas a uma network ACL.

Para determinar qual Network ACL está 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 Subnets e selecione a sub-rede.

   A Network ACL associada à sub-rede está incluída na guia Network ACL, junto com as regras da Network ACL.

Para determinar quais sub-redes estão associada a uma Network ACL

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

2. No painel de navegação, selecione Network ACLs. A coluna Associated With indica o número de sub-redes associadas para cada Network ACL.
3. Selecione uma Network ACL.
4. No painel de detalhes, escolha Subnet Associations (Associações de sub-redes) para exibir as sub-redes associadas à network ACL.

Criar uma network ACL

Você pode criar uma Network ACL personalizada para sua VPC. Por padrão, a Network ACL criada bloqueia todo tráfego de entrada e saída até o momento em que você adiciona regras, e ela será associada à sub-rede somente quando você a associar explicitamente a uma.

Para criar uma Network ACL

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Network ACLs.
3. Escolha Create Network ACL.
4. Na caixa de diálogo Create Network ACL (Criar network ACL), você tem a opção de nomear ou não sua Network ACL. Depois, selecione o ID de sua VPC na lista VPC. Depois, escolha Yes, Create (Sim, criar).

Adicionar e excluir regras

Quando você adiciona ou exclui uma regra de uma ACL, todas as sub-redes associadas à ACL ficam sujeitas a essa alteração. Não é necessário encerrar e reiniciar as instâncias na sub-rede. As alterações entram em vigor após um curto período.

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 Network ACL

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Network ACLs.
3. No painel de detalhes, escolha a guia Inbound Rules ou Outbound Rules, dependendo do tipo de regra que você necessita adicionar, e depois escolha Edit.
4. Em Rule #, insira um número de regra (por exemplo, 100). O número da regra não pode estar sendo usado na network ACL. Processamos as regras sequencialmente, a partir do 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.
5. Selecione uma regra na lista Type. Por exemplo, para adicionar uma regra para HTTP, escolha HTTP. Para adicionar uma regra para permitir todos os tráfegos TCP, escolha All TCP. Para algumas dessas opções (por exemplo, HTTP), preenchemos a porta para você. Para usar um protocolo que não esteja listado, escolha Custom Protocol Rule.
6. (Opcional) Se você estiver criando uma regra de protocolo personalizada, selecione o número e o nome do protocolo na lista Protocol. Para obter mais informações, consulte IANA List of Protocol Numbers.

7. (Opcional) Se o protocolo que você selecionou exigir um número de porta, insira o número de porta ou o intervalo de portas separadas por hífen (por exemplo, 49152-65535).
8. No campo Source ou Destination (dependendo se a regra for de entrada ou de saída), insira o intervalo CIDR ao qual a regra se aplica.
9. Na lista Allow/Deny, selecione ALLOW para permitir um tráfego específico ou DENY para negar um tráfego específico.
10. (Opcional) Para adicionar outra regra, escolha Add another rule e repita as etapas 4 a 9, se necessário.
11. Quando concluir, selecione Save.

Para excluir uma regra de uma Network ACL

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, selecione a guia Inbound Rules ou Outbound Rules e escolha Edit. Escolha Remove para a regra que você deseja excluir e depois Save.

Associar uma sub-rede a uma network ACL

Para aplicar as regras de uma Network ACL a uma sub-rede específica, você deve associar a sub-rede a uma Network ACL. É possível associar uma network ACL a várias sub-redes. No entanto, uma sub-rede pode ser associada a apenas uma network ACL. Por padrão, as sub-redes não associadas a uma ACL específica são associadas à network ACL padrão.

Para associar uma sub-rede a uma Network ACL

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 Associate para a sub-rede associada à Network ACL e escolha Save.

Desassociar uma network ACL de uma sub-rede

É possível desassociar uma network ACL personalizada de uma sub-rede. Quando a sub-rede tiver sido desassociada da network ACL personalizada, ela será automaticamente associada à network ACL padrão.

Para dissociar uma sub-rede de uma Network ACL

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, escolha a guia Subnet Associations.
4. Escolha Edit e desmarque a caixa de seleção Associate para a sub-rede. Escolha Save (Salvar).

Alterar a network ACL de uma sub-rede

Você pode mudar a Network ACL que está associada a uma sub-rede. Por exemplo, quando se cria uma sub-rede, a princípio ela é associada à Network ACL padrão. Em vez disso, você pode querer associá-la a uma Network ACL personalizada que tenha criado.

Depois de alterar a network ACL de uma sub-rede, você não precisa encerrar e reiniciar as instâncias na sub-rede. As alterações entram em vigor após um curto período.

Para mudar a associação de uma Network ACL a uma sub-rede

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. Escolha a guia Network ACL e depois Edit.
4. Na lista Change to (Alterar para), selecione a network ACL à qual associar a sub-rede e, depois, escolha Save (Salvar).

Excluir uma network ACL

Você poderá excluir uma Network ACL somente se não houver nenhuma sub-rede associada a ela. Não é possível excluir a Network ACL padrão.

Para excluir uma Network ACL

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 Network ACL e escolha Delete.
4. Na caixa de diálogo de confirmação, escolha Yes, Delete.

Visão geral da API e dos comandos

Você pode executar as tarefas descritas nesta página usando a linha de comando ou uma API. Para obter mais informações sobre as interfaces de linha de comando e uma lista das APIs disponíveis, consulte Acessar a Amazon VPC (p. 1).

Criar uma Network ACL para sua VPC

- create-network-acl (CLI da AWS)
- New-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Descrever uma ou mais de suas Network ACLs

- describe-network-acls (CLI da AWS)
- Get-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Adicionar uma regra a uma Network ACL

- create-network-acl-entry (CLI da AWS)
- New-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Excluir uma regra de uma Network ACL

- delete-network-acl-entry (CLI da AWS)
- Remove-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Substituir uma regra existente em uma Network ACL

- replace-network-acl-entry (CLI da AWS)
- Set-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Substituir uma associação de Network ACL

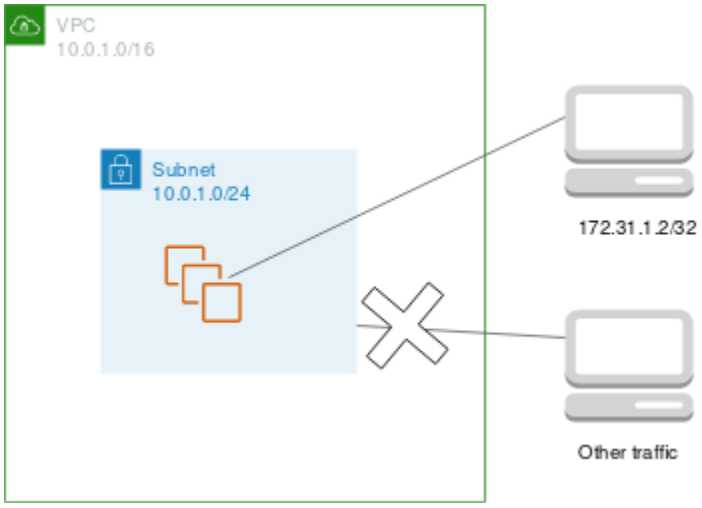
- replace-network-acl-association (CLI da AWS)
- Set-EC2NetworkAclAssociation (AWS Tools for Windows PowerShell)

Excluir uma Network ACL

- delete-network-acl (CLI da AWS)
- Remove-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Exemplo: Controlar o acesso a instâncias em uma sub-rede

Neste exemplo, as instâncias em sua sub-rede podem se comunicar entre si e são acessíveis de um computador remoto confiável. O computador remoto pode ser um computador em sua rede local ou uma instância em outra sub-rede ou VPC. Você o usa para se conectar às instâncias a fim de executar tarefas administrativas. As regras de seu security group e as regras da Network ACL permitem acesso do endereço IP em seu computador remoto (172.31.1.2/32). Todo o outros tráfego proveniente da Internet ou de outras redes é negado.



Todas as instâncias usam o mesmo security group (sg-1a2b3c4d), com as regras a seguir.

Regras de entrada

Tipo de protocolo	Protocolo	Intervalo de portas	Origem	Comentários
Todo o tráfego	Tudo	Tudo	sg-1a2b3c4d	Permite que as instâncias associadas ao mesmo grupo de segurança se comuniquem entre elas.
SSH	TCP	22	172.31.1.2/32	Permite acesso SSH de entrada

				do computador remoto. Se a instância for um computador Windows, essa regra deverá usar o protocolo RDP para a porta 3389.

Regras de saída

Tipo de protocolo	Protocolo	Intervalo de portas	Destino	Comentários
Todo o tráfego	Tudo	Tudo	sg-1a2b3c4d	Permite que as instâncias associadas ao mesmo grupo de segurança se comuniquem entre elas. Os grupos de segurança são stateful. Portanto, você não precisa de uma regra que permita o tráfego de resposta para solicitações de entrada.

A sub-rede está associada a uma Network ACL que tem as regras a seguir.

Regras de entrada

Regra nº	Tipo	Protocolo	Intervalo de portas	Origem	Permissão/ Negação	Comentários
100	SSH	TCP	22	172.31.1.2/32	PERMISSÃO	Permite tráfego de entrada do computador remoto. Se a instância for um computador Windows, essa regra deverá usar o protocolo RDP para a porta 3389.
*	Todo o tráfego	Tudo	Todos	0.0.0.0/0	NEGAÇÃO	Nega todos os outros tráfegos de entrada que não correspondem

						com a regra anterior.

Regras de saída

Regra nº	Tipo	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. Network ACLs são stateless. Portanto, essa regra é necessária para permitir o tráfego de resposta para solicitações de entrada.
*	Todo o tráfego	Tudo	Todos	0.0.0.0/0	NEGAÇÃO	Nega todos os outros tráfegos de saída que não correspondem com a regra anterior.

Nesse cenário, você tem flexibilidade para mudar as regras de um ou mais grupos de segurança de suas instâncias e ter a Network ACL como camada de defesa de backup. As regras de network ACL se aplicam a todas as instâncias na sub-rede. Se você acidentalmente tornar as regras do grupo de segurança permissivas demais, as regras de network ACL continuarão a permitir acesso apenas a partir do único endereço IP. Por exemplo, as regras a seguir são mais permissivas do que as regras anteriores: elas permitem acesso SSH de entrada de qualquer endereço IP.

Regras de entrada

Tipo	Protocolo	Intervalo de portas	Origem	Comentários
Todo o tráfego	Tudo	Tudo	sg-1a2b3c4d	Permite que as instâncias associadas ao mesmo grupo de segurança se comuniquem entre elas.
SSH	TCP	22	0.0.0.0/0	Permite acesso SSH de qualquer endereço IP.

Regras de saída

Tipo	Protocolo	Intervalo de portas	Destino	Comentários
Todo o tráfego	Tudo	Todos	0.0.0.0/0	Permite todos os tráfegos de saída.

Entretanto, somente outras instâncias dentro da sub-rede e seu computador remoto podem acessar essa instância. As regras de Network ACL ainda impedem todos os tráfegos de entrada à sub-rede, exceto o proveniente de seu computador remoto.

Regras recomendadas para cenários de assistente de VPC

É possível usar o assistente da VPC no console da Amazon VPC para implementar cenários comuns para a Amazon VPC. Se você implementar esses cenários conforme descrito na documentação, use a lista de controle de acesso (ACL) de rede padrão, que permite tráfego de entrada e de saída. Se precisar de uma extra de segurança, poderá criar uma Network ACL e adicionar regras. Para obter mais informações, consulte um dos seguintes:

- the section called “Regras de network ACL recomendadas para uma VPC com uma única sub-rede pública” (p. 27)
- the section called “Regras de network ACL recomendadas para uma VPC com sub-redes públicas e privadas (NAT)” (p. 40)
- the section called “Regras de network ACL recomendadas para uma VPC com sub-redes públicas e privadas e acesso à AWS Site-to-Site VPN” (p. 62)
- the section called “Regras de network ACL recomendadas para uma VPC com apenas uma sub-rede privada e acesso à AWS Site-to-Site VPN” (p. 77)

Melhores práticas de segurança para a VPC

As melhores práticas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas práticas recomendadas podem não ser adequadas ou suficientes no seu ambiente, trate-as como considerações úteis em vez de requisitos.

Veja a seguir as melhores práticas gerais:

- Use várias implantações de zona de disponibilidade para ter alta disponibilidade.
- Use grupos de segurança e network ACLs. Para obter mais informações, consulte Grupos de segurança para a VPC (p. 180) e Network ACLs (p. 190).
- Use políticas do IAM para controlar o acesso.
- Use o Amazon CloudWatch para monitorar seus componentes da VPC e conexões VPN.
- Use logs de fluxo para capturar informações sobre o tráfego IP de e para as interfaces de rede na VPC. Para obter mais informações, consulte VPC Flow Logs (p. 310).

Recursos adicionais

- Gerencie o acesso aos recursos e às APIs da AWS usando a federação de identidades, os usuários do IAM e as funções do IAM. Estabeleça políticas e procedimentos de gerenciamento de credenciais

para criar, distribuir, rotacionar e revogar credenciais de acesso da AWS. Para obter mais informações, consulte Melhores práticas do IAM no Guia do usuário do IAM.

- Para obter respostas às perguntas frequentes sobre segurança da VPC, consulte Perguntas frequentes da Amazon VPC.

Componentes das redes VPC

Você pode usar os componentes a seguir para configurar redes em sua VPC.

Componentes

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.

Um gateway da internet tem duas finalidades: fornecer um destino nas tabelas de rotas da VPC para o tráfego roteável na Internet e executar a network address translation (NAT - tradução de endereços de rede) para instâncias designadas com endereços IPv4 públicos. Para obter mais informações, consulte Habilitar o acesso à Internet (p. 212).

Um gateway da internet oferece suporte para tráfego IPv4 e IPv6. Não causa riscos de disponibilidade ou restrições de largura de banda no tráfego de rede. Não há custo adicional por ter um gateway da Internet na sua conta.

Habilitar o acesso à Internet

Para permitir acesso à Internet ou a partir dela para instâncias em uma sub-rede em uma VPC, proceda da seguinte forma:

- Crie um gateway de 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 IP exclusivo globalmente (endereço IPv4 público, endereço IP elástico ou endereço IPv6).
- Certifique-se de que as listas de controle de acesso da rede e as regras do grupo de segurança permitam que o tráfego relevante flua para e da instância.

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.

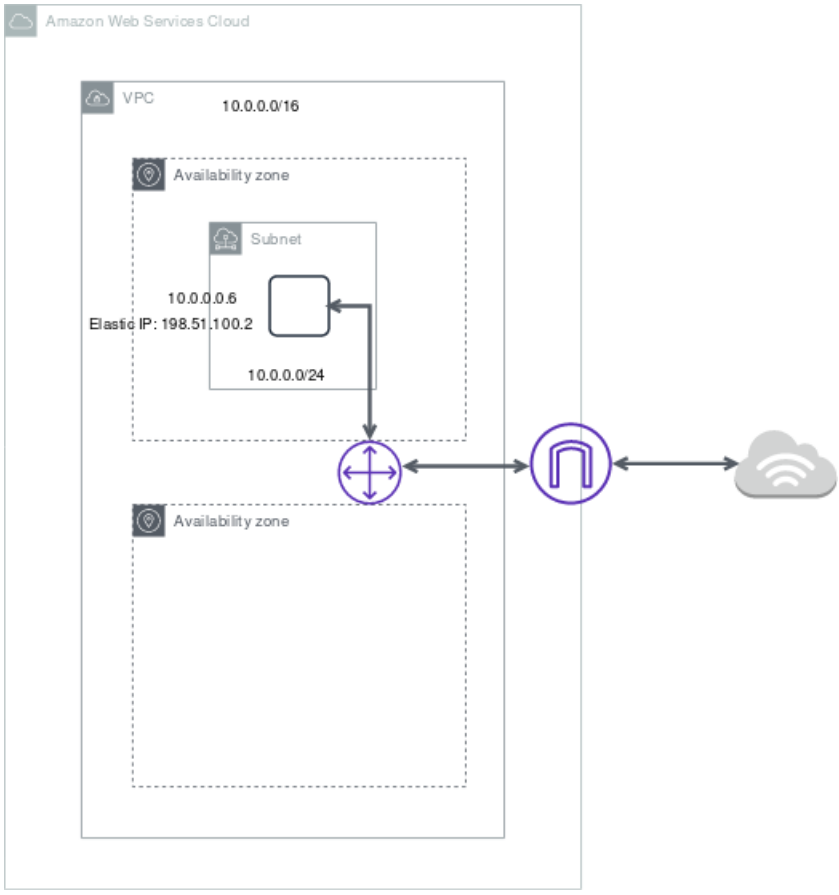
Na tabela de rotas da sub-rede pública, é possível especificar uma rota para o gateway da Internet para todos os destinos não explicitamente conhecidos pela tabela de rotas (`0.0.0.0/0` para IPv4 ou `::/0` para IPv6). Como alternativa, avalie a rota para uma gama mais restrita de endereços IP, por exemplo, 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 público IPv4 ou um endereço IP elástico que esteja associado a um endereço IPv4 privado na instância. 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 1 na VPC é uma sub-rede pública. Ela está associada a uma tabela de rotas personalizada que aponta todo o tráfego IPv4 vinculado à internet para um gateway da Internet. A instância possui um endereço IP elástico que permite a comunicação com a internet.



Para fornecer às instâncias acesso à Internet sem atribuir endereços IP públicos, é possível usar 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 obter mais informações, consulte Dispositivos NAT para sua VPC (p. 228).

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	É possível criar a VPC usando a primeira ou a segunda opção no assistente VPC. Caso contrário, crie e anexe manualmente o gateway da internet.
Tabela de rotas com rota para o gateway da internet para tráfego IPv4 (0.0.0.0/0)	Sim	É possível criar a VPC usando a primeira ou a segunda opção no assistente VPC. Caso contrário, crie manualmente a tabela de rotas e adicione a rota.
Tabela de rotas com rota para o gateway da internet para tráfego IPv6 (::/0)	Não	É possível criar a VPC usando a primeira ou a segunda opção no assistente VPC, além de especificar a opção para associar um bloco CIDR IPv6 à VPC. Caso contrário, crie manualmente a tabela de rotas e adicione a rota.
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 VPC e sub-redes padrão (p. 149). Para obter mais informações sobre como usar o assistente de VPC para criar uma VPC com um gateway da internet, consulte VPC com uma única sub-rede pública (p. 20) ou VPC com sub-redes públicas e privadas (NAT) (p. 31).

Para obter mais informações sobre o endereçamento IP na VPC e sobre o controle da atribuição de endereços públicos IPv4 ou IPv6 às instâncias, consulte Endereçamento IP na sua VPC (p. 117).

Ao adicionar uma nova sub-rede à VPC, é preciso configurar o roteamento e a segurança desejada para a sub-rede.

Adicionar um gateway da Internet à VPC.

As seções a seguir descrevem como criar manualmente uma sub-rede pública e anexar um gateway da Internet à VPC a fim de oferecer suporte ao acesso à Internet.

Tarefas

Criar uma sub-rede

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 Subnets (Sub-redes), Create Subnet (Criar sub-rede).
3. Especifique os detalhes da sub-rede conforme necessário:
   - Name tag (Tag de nome): opcionalmente, forneça um nome para sua sub-rede. Ao fazer isso, é criada uma tag com a chave `Name` e o valor especificado.
   - VPC: Escolha a VPC na qual você está criando a sub-rede.
   - Availability Zone (Zona de disponibilidade): opcionalmente, escolha uma zona de disponibilidade ou uma zona local na qual sua sub-rede residirá ou deixe o padrão No Preference (Sem preferência) para permitir que a AWS escolha uma zona de disponibilidade para você.

     Para obter informações sobre as regiões que oferecem suporte a zonas locais, consulte Regiões disponíveis no Guia do usuário do Amazon EC2 para instâncias do Linux.
   - Bloco CIDR IPv4: Especifique um bloco CIDR IPv4 para sua sub-rede, por exemplo, `10.0.1.0/24`. Para obter mais informações, consulte Dimensionamento da VPC e da sub-rede para IPv4 (p. 103).
   - Bloco CIDR IPv6: (Opcional) Se você associou um bloco CIDR IPv6 a sua VPC, selecione Especificar um CIDR IPv6 personalizado. Especifique o valor do par hexadecimal para a sub-rede ou mantenha o valor padrão.
4. Escolha Create (Criar).

Para obter mais informações sobre sub-redes, consulte VPCs e sub-redes (p. 100).

Criar e associar de um gateway da Internet

Depois de criar um gateway da Internet, anexe-o à VPC

Para criar um gateway da internet e anexá-lo à 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) e selecione Create internet gateway (Criar gateway da internet).
3. Opcionalmente, atribua um nome ao gateway da Internet.
4. Opcionalmente, adicione ou remova uma tag.

   [Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:
   - Em Key (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. Escolha Criar gateway da Internet.
6. Selecione o gateway da internet criado e escolha Actions, Attach to VPC (Ações, anexar à VPC).
7. Selecione a VPC na lista e escolha Anexar gateway da Internet.

Criar uma tabela de rotas personalizada

Ao criar uma sub-rede, nós a associamos automaticamente à tabela de rotas principais para a VPC. Por padrão, a tabela de rotas principal não contém uma rota para um gateway da internet. O procedimento a seguir cria uma tabela de rotas personalizada com uma rota que envia o tráfego destinado para fora da VPC para o gateway da internet e, em seguida, associa a rota à sub-rede.

Para criar uma tabela de rotas personalizada

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Route Tables e selecione Create Route Tables.
3. Na caixa de diálogo Create Route Table, atribua um nome, opcionalmente, à tabela de rotas e selecione a VPC e Yes, Create.
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, selecione Edit, Add another route e adicione as rotas, conforme necessário. Selecione Save (Salvar) ao concluir.
   - Para o tráfego IPv4, especifique `0.0.0.0/0` na caixa Destination (Destino) e selecione o ID do gateway da internet na lista Target (Destino).
   - Para o tráfego IPv6, especifique `::/0` na caixa Destination (Destino) e selecione o ID do gateway da internet na lista Target (Destino).
6. Na guia Subnet Associations, escolha Edit, selecione a caixa de seleção Associate para a sub-rede e escolha Save.

Para obter mais informações, consulte Tabelas de rotas para sua VPC (p. 283).

Criar um grupo de segurança para acesso à Internet

Por padrão, um grupo de segurança da VPC permite todo o tráfego de saída. É possível criar um grupo de segurança e adicionar regras que permitam tráfego de entrada da Internet. Depois, associe o grupo de segurança a instâncias na sub-rede pública.

Criar um novo security group e associá-lo às instâncias

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Security Groups (Grupos de segurança), Create Security Group (Criar grupo de segurança).
3. Na caixa de diálogo Create Security Group, especifique um nome para o security group e forneça uma descrição. Selecione o ID na lista VPC e, então, escolha Yes, Create.
4. Selecione o security group. O painel de detalhes exibe informações sobre o security group, assim como guias para trabalhar com as respectivas regras de entrada e saída.
5. Na guia Inbound Rules, escolha Edit. Escolha Add Rule (Adicionar regra) e complete as informações necessárias. Por exemplo, selecione HTTP ou HTTPS na lista Type e, em Source, digite `0.0.0.0/0` para o tráfego IPv4 ou `::/0` para o tráfego IPv6. Selecione Save (Salvar) ao concluir.

6. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
7. No painel de navegação, escolha Instances (Instâncias).
8. Selecione a instância, depois Actions e Redes. Escolha Change Security Groups.
9. Na caixa de diálogo Change Security Groups, desmarque o security group da caixa de seleção e escolha um novo. Escolha Assign Security Groups.

Para obter mais informações, consulte Grupos de segurança para a VPC (p. 180).

Adicionar endereços IP elásticos

Depois de executar uma instância na sub-rede, atribua um endereço IP elástico a ela, se desejar que ela seja acessível pela internet por meio do IPv4.

> Note
>
> Se você tiver atribuído um endereço IPv4 público à instância durante a execução, a instância será acessível na internet, e você não precisará atribuir um endereço IP elástico. Para obter mais informações sobre o endereçamento IP para a instância, consulte Endereçamento IP na sua VPC (p. 117).

Para alocar um endereço IP elástico e atribuí-lo a uma instância usando o console

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 Allocate new address.
4. Escolha Allocate.

   > Note
   >
   > Se sua conta for compatível com o EC2-Classic, escolha primeiro VPC.
5. Selecione o endereço IP elástico na lista, selecione Actions (Ações) e Associate address (Associar endereço).
6. 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 que será associado ao endereço IP elástico e, então, escolha Associar.

Para obter mais informações, consulte Endereços IP elásticos (p. 277).

Separar um gateway da Internet da VPC

Se não precisar mais de acesso à Internet para as instâncias executadas em uma VPC não padrão, 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 desanexar um gateway da internet

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Elastic IPs e selecione Elastic IP address.
3. Escolha Actions e Disassociate address. Escolha Disassociate-address.
4. No painel de navegação, escolha Gateways da Internet.
5. Selecione o gateway da internet e escolha Actions, Detach from VPC (Ações, Desanexar da VPC).
6. Na caixa de diálogo Desanexar da VPC, escolha Desanexar gateway da Internet.

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 Gateways da Internet.
3. Selecione o gateway da internet e escolha Actions (Ações), Delete internet gateway (Excluir gateway da internet).
4. Na caixa de diálogo Excluir gateway da Internet, insira `delete` e escolha Excluir gateway da Internet.

Visão geral da API e dos comandos

Você pode executar as tarefas descritas nesta página 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 Acessar a Amazon VPC (p. 1).

Criar um gateway da internet

- create-internet-gateway (CLI da AWS)
- New-EC2InternetGateway (AWS Tools for Windows PowerShell)

Anexar um gateway da internet a uma VPC

- attach-internet-gateway (CLI da AWS)
- Add-EC2InternetGateway (AWS Tools for Windows PowerShell)

Descrever um gateway da internet

- describe-internet-gateways (CLI da AWS)
- Get-EC2InternetGateway (AWS Tools for Windows PowerShell)

Desanexar um gateway da Internet de uma VPC

- detach-internet-gateway (CLI da AWS)
- Dismount-EC2InternetGateway (AWS Tools for Windows PowerShell)

Excluir um gateway da internet

- delete-internet-gateway (CLI da AWS)
- Remove-EC2InternetGateway (AWS Tools for Windows PowerShell)

Gateways da Internet apenas 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.

Note

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 obter mais informações, consulte Gateways NAT (p. 229).

Tópicos

Noções básicas do Gateway da Internet somente de saída

Uma instância na sub-rede pública pode se conectar à Internet pelo gateway da Internet se tiver um endereço IPv4 ou um endereço IPv6 público. Da mesma forma, os recursos na Internet podem iniciar uma conexão com a instância usando o endereço IPv4 ou o endereço IPv6 público; por exemplo, quando você se conecta à instância usando seu computador local.

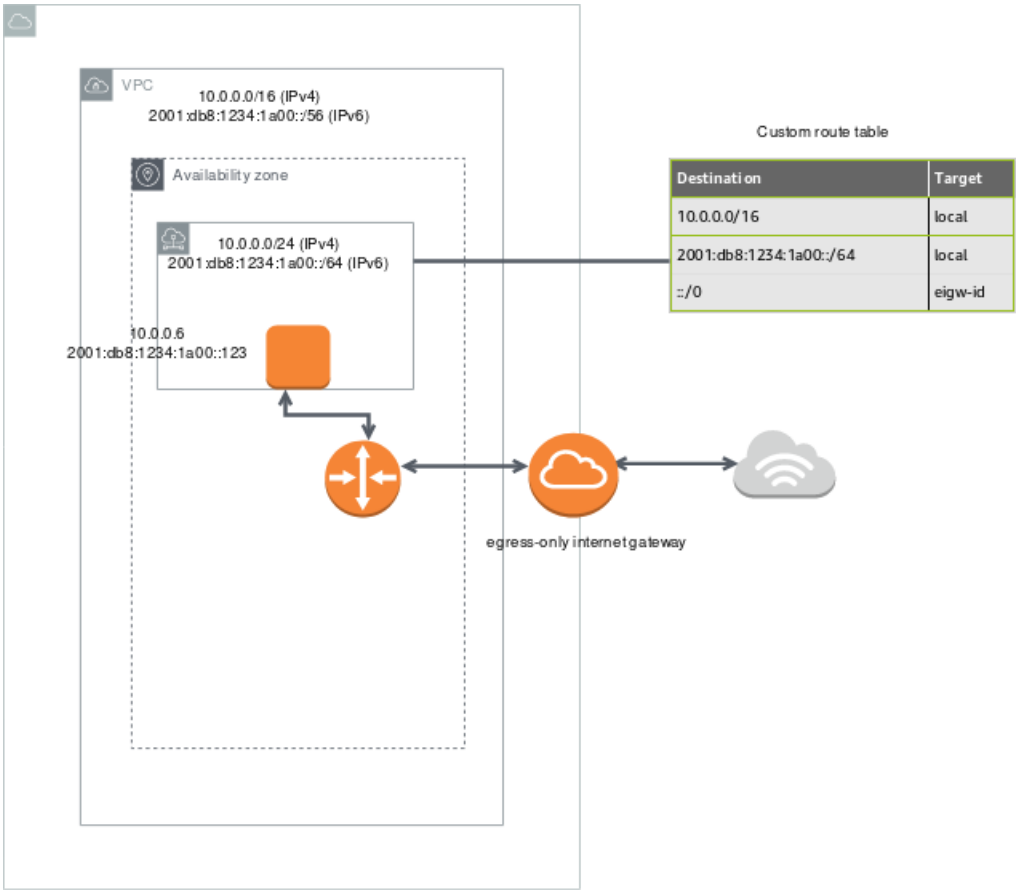
Os endereços IPv6 são exclusivos globalmente e, são portanto, públicos por padrão. Se deseja que a instância possa acessar a Internet, mas deseja impedir que recursos na Internet iniciem a comunicação com a instância, será possível usar um gateway da Internet somente de saída. Para fazer isso, crie um 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 do tipo com estado: encaminha o tráfego das instâncias da sub-rede para a Internet ou outros serviços da AWS e envia a resposta de volta às instâncias.

Um gateway da Internet somente de saída possui as seguintes características:

- Não é possível associar um grupo de segurança a um gateway da Internet somente de saída. Você pode usar security groups para suas instâncias na sub-rede privada para controlar o tráfego de entrada e saída dessas instâncias.
- 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, uma VPC possui um bloco CIDR IPv6 e uma sub-rede na VPC possui um bloco CIDR IPv6. Uma tabela de rotas personalizada está associada à sub-rede 1 e aponta todo o tráfego IPv6 vinculado à Internet (`::/0`) para um gateway da Internet somente de saída na VPC.



Trabalhar com os gateways da Internet somente de saída

As seções a seguir descrevem como criar um gateway da Internet somente de saída para a sub-rede privada e configurar o roteamento da sub-rede.

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 Key (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 Create (Criar).

Visualizar o gateway da Internet somente de saída

É possível criar um gateway da Internet somente de saída no console da Amazon VPC.

Como ver informações sobre 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, selecione Gateways da Internet somente de saída.
3. Selecione o gateway da Internet somente de saída para visualizar suas informações no painel de detalhes.

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 Tabelas de rotas, Criar rotas.
3. Na caixa de diálogo Criar tabela de rotas, atribua, opcionalmente, um nome à tabela de rotas, selecione a VPC e escolha Sim, criar.
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 (Editar), especifique `::/0` na caixa Destination (Destino), selecione o ID do gateway da Internet na lista Target (Destino) e Save (Salvar).
6. Na guia Associações de sub-rede, escolha Editar e marque a caixa de seleção Associar da 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 Tabelas de rotas para sua VPC (p. 283).

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.
4. Selecione Delete Egress Only Internet Gateway na caixa de diálogo de confirmação.

Visão geral da API e da CLI

Você pode executar as tarefas descritas nesta página 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 Acessar a Amazon VPC (p. 1).

Criar um gateway da Internet somente de saída

- create-egress-only-internet-gateway (CLI da AWS)
- New-EC2EgressOnlyInternetGateway (AWS Tools for Windows PowerShell)

Descrever um gateway da Internet somente de saída

- describe-egress-only-internet-gateways (CLI da AWS)
- Get-EC2EgressOnlyInternetGatewayList (AWS Tools for Windows PowerShell)

Excluir um gateway da Internet somente de saída

- delete-egress-only-internet-gateway (CLI da AWS)
- Remove-EC2EgressOnlyInternetGateway (AWS Tools for Windows PowerShell)

Gateways de operadora

Um gateway de operadora tem duas finalidades. Ele permite o tráfego de entrada de uma rede de operadora em um local específico e o tráfego de saída para a rede de operadora e a Internet. Não há configuração de conexão de entrada da Internet para uma zona do Wavelength por meio do gateway de operadora.

Um gateway de operadora oferece suporte a tráfego IPv4.

Os gateways de operadora só estão disponíveis para VPCs que contêm sub-redes em uma zona do Wavelength. O gateway de operadora fornece conectividade entre a zona do Wavelength, a operadora de telecomunicações e os dispositivos na rede da operadora de telecomunicações. O gateway de operadora executa o NAT dos endereços IP das instâncias do Wavelength para os endereços IP da operadora de um grupo atribuído ao grupo de borda de rede. A função NAT do gateway de operadora é semelhante à forma como um gateway da Internet funciona em uma região.

Habilitar o acesso à rede de operadoras de telecomunicações

Para habilitar o acesso à rede da operadora de telecomunicações para instâncias em uma sub-rede do Wavelength e vice-versa, é necessário fazer o seguinte:

- Crie uma VPC.
- Crie um gateway de operadora e conecte-o à VPC. Ao criar o gateway de operadora, é possível escolher quais sub-redes são roteadas para ele. Ao selecionar essa opção, criamos automaticamente os recursos relacionados aos gateways de operadora, como tabelas de rotas e network ACLs. Se não escolher essa opção, será necessário executar as seguintes tarefas:
  - Selecione as sub-redes que roteiam o tráfego para o gateway de operadora.
  - Verifique se as tabelas de rotas de sub-rede têm uma rota que direciona o tráfego para o gateway de operadora.

- Verifique se as instâncias em sua sub-rede têm um endereço IP de operadora globalmente exclusivo.
- Certifique-se de que as listas de controle de acesso da rede e as regras do grupo de segurança permitam que o tráfego relevante flua para e da instância.

Trabalhar com gateways de operadora

As seções a seguir descrevem como criar manualmente um gateway de operadora para a VPC a fim de oferecer suporte ao tráfego de entrada da rede da operadora (por exemplo, celulares) e ao tráfego de saída para a rede da operadora e a Internet.

Tarefas

Criar uma VPC

É possível criar uma VPC do Wavelength vazia usando o console da Amazon VPC ou a CLI da AWS.

Amazon VPC 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), Create VPC (Criar VPC).
3. Especifique os seguintes detalhes da VPC conforme necessário e selecione Create (Criar).
   - Name tag (Tag do nome): opcionalmente, forneça um nome para a sua VPC. Ao fazer isso, é criada uma tag com a chave `Name` e o valor especificado.
   - Bloco CIDR IPv4: Especifique um bloco CIDR IPv4 para sua VPC. Recomendamos que você especifique um bloco CIDR a partir dos intervalos de endereços IP privados (não roteados publicamente) conforme especificado em RFC 1918; por exemplo, `10.0.0.0/16` ou `192.168.0.0/16`.

     Note

     É possível especificar um intervalo de endereços IPv4 publicamente roteáveis. No entanto, atualmente não oferecemos suporte para acesso direto à Internet de blocos CIDR publicamente roteáveis em uma VPC. As instâncias do Windows não podem inicializar corretamente se forem executadas em uma VPC com intervalos de `224.0.0.0` a `255.255.255.255` (intervalos de endereço IP de classe D e classe E).

AWS CLI

Para criar uma VPC

- Use `create-vpc`. Para obter mais informações, consulte create-vpc na Referência de comando da CLI da AWS.

Criar um gateway de operadora

Depois de criar uma VPC, crie um gateway de operadora e selecione as sub-redes que roteiam o tráfego para ele.

Se não aceitou uma zona do Wavelength, o console da Amazon VPC solicitará que você aceite. Para obter mais informações, consulte the section called “Gerenciar zonas” (p. 228).

Ao escolher rotear automaticamente o tráfego de sub-redes para o gateway de operadora, criamos os seguintes recursos:

- Um gateway de operadora.
- Uma sub-rede. É possível atribuir todas as tags de gateway de operadora que não têm um valor de Key (Chave) de `Name` para a sub-rede.
- Uma network ACL com os seguintes recursos:
  - Uma sub-rede associada à sub-rede na zona do Wavelength
  - Regras padrão de entrada e saída para todo o tráfego.
- Uma tabela de rotas com os seguintes recursos:
  - Uma rota para todo o tráfego local
  - Uma rota que roteia todo o tráfego não local para o gateway de operadora
  - Uma associação com a sub-rede

Amazon VPC console

Como criar um gateway de operadora

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Carrier Gateways (Gateways de operadora) e escolha Create carrier gateway (Criar gateway de operadora).
3. Opcional: Em Name (Nome), insira um nome para o gateway de operadora.
4. Em VPC, escolha a VPC.
5. Escolha Route subnet traffic to carrier gateway (Encaminhar tráfego de sub-rede para o gateway de operadora) e, em Subnets to route (Sub-redes a serem roteadas), faça o seguinte.

   a. Em Existing subnets in Wavelength Zone (Sub-redes existentes na zona do Wavelength), selecione a caixa de cada sub-rede a ser roteada para o gateway de operadora.

   b. Para criar uma sub-rede na zona do Wavelength, escolha Add new subnet (Adicionar nova sub-rede), especifique as seguintes informações e escolha Add new subnet (Adicionar nova sub-rede):

      - Name tag (Tag de nome): opcionalmente, forneça um nome para sua sub-rede. Ao fazer isso, é criada uma tag com a chave `Name` e o valor especificado.
      - VPC: escolha a VPC.
      - Availability Zone (Zona de disponibilidade): escolha a zona do Wavelength.
      - Bloco CIDR IPv4: Especifique um bloco CIDR IPv4 para sua sub-rede, por exemplo, `10.0.1.0/24`.
      - Para aplicar as tags do gateway de operadora à sub-rede, selecione Apply same tags from this carrier gateway (Aplicar as mesmas tags deste gateway de operadora).
6. (Opcional) Para adicionar uma tag ao gateway de operadora, escolha Add tag (Adicionar tag) e faça o seguinte:
   - Em Key (Chave), insira o nome da chave.
   - Em Value (Valor), insira o valor da chave.

7. Escolha Create carrier gateway (Criar gateway de operadora).

AWS CLI

Como criar um gateway de operadora

- Use `create-carrier-gateway`. Para obter mais informações, consulte create-carrier-gateway na Referência de comando da CLI da AWS.

  Depois de criar o gateway de operadora, adicione uma tabela de rotas da VPC com os seguintes recursos:

  - Uma rota para todo o tráfego local da VPC
  - Uma rota que roteia todo o tráfego não local para o gateway de operadora
  - Uma associação com as sub-redes na zona do Wavelength

  Para obter mais informações, consulte the section called “Rotear para um gateway de operadora de zona do Wavelength” (p. 293) e the section called “Trabalhar com tabelas de rotas” (p. 301).

Criar um grupo de segurança para acessar a rede de operadoras de telecomunicações

Por padrão, um grupo de segurança da VPC permite todo o tráfego de saída. É possível criar um grupo de segurança e adicionar regras que permitam tráfego de entrada da operadora de telecomunicações. Associe o grupo de segurança às instâncias na sub-rede.

Amazon VPC console

Criar um novo security group e associá-lo às instâncias

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Security Groups (Grupos de segurança), Create Security Group (Criar grupo de segurança).
3. Para criar um grupo de segurança, escolha Create security group (Criar grupo de segurança), especifique as seguintes informações e escolha create (criar):
   - Security group name (Nome do grupo de segurança): insira um nome para a sub-rede.
   - Description (Descrição): informe a descrição do grupo de segurança.
   - VPC: escolha a VPC.
4. Selecione o security group. O painel de detalhes exibe informações sobre o security group, assim como guias para trabalhar com as respectivas regras de entrada e saída.
5. Na guia Inbound Rules, escolha Edit. Escolha Add Rule (Adicionar regra) e complete as informações necessárias. Por exemplo, selecione HTTP ou HTTPS na lista Type e, em Source, digite `0.0.0.0/0` para o tráfego IPv4 ou `::/0` para o tráfego IPv6. Escolha Salvar.
6. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
7. No painel de navegação, escolha Instances (Instâncias).
8. Selecione a instância, escolha Actions (Ações) e Networking (Redes) e selecione Change Security Groups (Alterar grupos de segurança).
9. Desmarque a caixa de seleção do grupo de segurança selecionado no momento e selecione o novo. Escolha Assign Security Groups.

AWS CLI

Para criar um security group

- Use `create-security-group`. Para obter mais informações, consulte create-security-group na Referência de comando da CLI da AWS.

Alocar e associar um endereço IP de operadora à instância na sub-rede da zona do Wavelength

Se você usou o console do Amazon EC2 para executar a instância ou não usou a opção `associate-carrier-ip-address` na CLI da AWS, será necessário alocar um endereço IP de operadora e atribuí-lo à instância:

Como alocar e associar um endereço IP de operadora

1. Use `allocate-address` para alocar um endereço IP de operadora. Para obter mais informações, consulte allocate-address na Referência de comando da CLI da AWS.

   Exemplo

   ```
   aws ec2 allocate-address --region us-east-1 --domain vpc --network-border-group us-
   east-1-wl1-bos-wlz-1
   ```

   Resultado

   ```
   {
       "AllocationId": "eipalloc-05807b62acEXAMPLE",
       "PublicIpv4Pool": "amazon",
       "NetworkBorderGroup": "us-east-1-wl1-bos-wlz-1",
       "Domain": "vpc",
       "CarrierIp": "155.146.10.111"

   }
   ```

2. Use `associate-address` para associar o endereço IP de operadora à instância do EC2. Para obter mais informações, consulte associate-address na Referência de comando da CLI da AWS.

   Exemplo

   ```
   aws ec2 associate-address --allocation-id eipalloc-05807b62acEXAMPLE --network-
   interface-id eni-1a2b3c4d
   ```

   Resultado

   ```
   {
       "AssociationId": "eipassoc-02463d08ceEXAMPLE",
   }
   ```

Exibir os detalhes do gateway de operadora

É possível visualizar informações sobre o gateway de operadora, inclusive o estado e as tags.

Amazon VPC console

Como visualizar os detalhes do gateway de operadora

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Carrier Gateways (Gateways de operadora).
3. Selecione o gateway de operadora e escolha Actions (Ações), View details (Visualizar detalhes).

AWS CLI

Como visualizar os detalhes do gateway de operadora

- Use `describe-carrier-gateways`. Para obter mais informações, consulte describe-carrier-gateways na Referência de comando da CLI da AWS.

Gerenciar tags de gateway de operadora

As tags ajudam você a identificar os gateways de operadora. É possível adicionar ou remover tags.

Amazon VPC console

Como gerenciar as tags do gateway de operadora

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Carrier Gateways (Gateways de operadora).
3. Selecione o gateway de operadora e escolha Actions (Ações), Manage tags (Gerenciar tags).
4. Para adicionar uma tag, escolha Add tag (Adicionar tag) e faça o seguinte:
   - Em Key (Chave), insira o nome da chave.
   - Em Value (Valor), insira o valor da chave.
5. Para remover uma tag, escolha Remove (Remover) à direita da chave e do valor da tag.
6. Escolha Save (Salvar).

AWS CLI

Como gerenciar as tags do gateway de operadora

- Para criar uma tag, use `create-tag`. Para obter mais informações, consulte create-tag na Referência de comando da CLI da AWS.

  Para excluir tags, use `delete-tags`. Para obter mais informações, consulte delete-tags na Referência de comando da CLI da AWS.

Excluir um gateway de operadora

Caso não precise mais de um gateway de operadora, é possível excluí-lo.

Important

Se você não excluir a rota que tem o gateway de operadora como Target (Destino), a rota será uma rota de buraco negro.

Amazon VPC console

Como excluir um gateway de operadora

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Carrier Gateways (Gateways de operadora).
3. Selecione o gateway de operadora e escolha Actions (Ações), Delete carrier gateway (Excluir gateway de operadora).
4. Na caixa de diálogo Delete carrier gateway (Excluir gateway de operadora), insira Delete (Excluir) e selecione Delete (Excluir).

AWS CLI

Como excluir um gateway de operadora

- Use `delete-carrier-gateway`. Para obter mais informações, consulte delete-carrier-gateway na Referência de comando da CLI da AWS.

Gerenciar zonas

Antes de especificar uma zona do Wavelength para um recurso ou um serviço, você deve ativar essa zona.

É necessário solicitar acesso para usar as zonas do Wavelength antes da ativação. Para obter informações sobre como solicitar acesso a zonas do Wavelength, consulte AWS Wavelength.

Dispositivos NAT para sua VPC

É possível usar um dispositivo NAT para permitir que instâncias em uma sub-rede privada se conectem à Internet (por exemplo, para atualizações de software) ou a outros serviços da AWS, mas evitar que a Internet inicie uma conexão com essas instâncias. O dispositivo NAT encaminha o tráfego para as instâncias na sub-rede privada para a Internet ou outros serviços da AWS e depois envia a resposta de volta às instâncias. Quando o tráfego é encaminhado para a Internet, o endereço IPv4 de origem é substituído pelo endereço do dispositivo NAT; do mesmo modo, quando a o tráfego de resposta volta para essas instâncias, o dispositivo NAT converte o endereço de volta nos endereços IPv4 privados dessas instâncias.

Os dispositivos NAT não são compatíveis com tráfego IPv6, use um gateway da Internet apenas de saída em vez disso. Para obter mais informações, consulte Gateways da Internet apenas de saída (p. 218).

Note

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 NAT gerenciado oferecido pela AWS chamado gateway NAT ou criar seu próprio dispositivo NAT em uma instância do EC2, chamado instância NAT. Recomendamos os gateways NAT porque eles oferecem maior disponibilidade e largura de banda do que as instâncias NAT. O serviço de gateway NAT é também um serviço gerenciado que não requer trabalho de administração.

Tópicos

- Comparação entre gateways NAT e instâncias NAT (p. 255)

AMI NAT (fim do suporte)

O AMI NAT é construído com base na última versão do Amazon Linux, 2018.03, que chegou ao fim do suporte padrão em 31 de dezembro de 2020. Para obter mais informações, consulte a seguinte postagem no blog: Fim da vida útil do Amazon Linux AMI. Esse recurso só receberá atualizações críticas de segurança (não haverá atualizações regulares).

Se você usar uma AMI NAT existente, a AWS recomenda migrar para um gateway NAT ou criar sua própria AMI NAT no Amazon Linux 2 o mais rápido possível. Para obter informações sobre como migrar sua instância, consulte the section called “Migrar de uma instância NAT” (p. 231).

Gateways NAT

É possível usar um gateway de conversão de endereços de rede (NAT) para permitir que instâncias em uma sub-rede privada se conectem à internet ou a outros serviços da AWS, mas evitar que a internet inicie uma conexão com essas instâncias. Para obter mais informações sobre NAT, consulte Dispositivos NAT para sua VPC (p. 228).

Você será cobrado para criar e usar um gateway NAT em sua conta. Serão aplicadas taxas de uso por hora do gateway NAT e de processamento de dados. Cobranças pela transferência de dados no Amazon EC2 também se aplicam. Para obter mais informações, consulte Definição de preço da Amazon VPC.

Os gateways NAT não são compatíveis com tráfego IPv6, use um gateway da Internet somente de saída em vez disso. Para obter mais informações, consulte Gateways da Internet apenas de saída (p. 218).

Tópicos

- Noções básicas de gateway NAT (p. 229)
- Trabalhar com gateways NAT (p. 232)
- Controlar o uso de gateways NAT (p. 235)
- Marcar um gateway NAT (p. 235)
- Visão geral da API e da CLI (p. 235)
- Monitorar gateways NAT usando o Amazon CloudWatch (p. 236)
- Solucionar problemas com gateways NAT (p. 241)

Noções básicas de gateway NAT

Para criar um gateway NAT, você deve especificar uma sub-rede pública na qual o gateway NAT residirá. Para obter mais informações sobre sub-redes públicas e privadas, consulte Roteamento de sub-rede (p. 108). Também é necessário especificar um endereço IP elástico (p. 277) para associá-lo com o gateway NAT ao criá-lo. O endereço IP elástico não poderá ser alterado depois que for associado ao gateway NAT. Depois que criar um gateway NAT, será necessário atualizar a tabela de rotas associada a uma ou mais de suas sub-redes privadas para direcionar o tráfego vinculado à Internet para o gateway NAT. Isso permite que as instâncias nas sub-redes privadas se comuniquem com a internet.

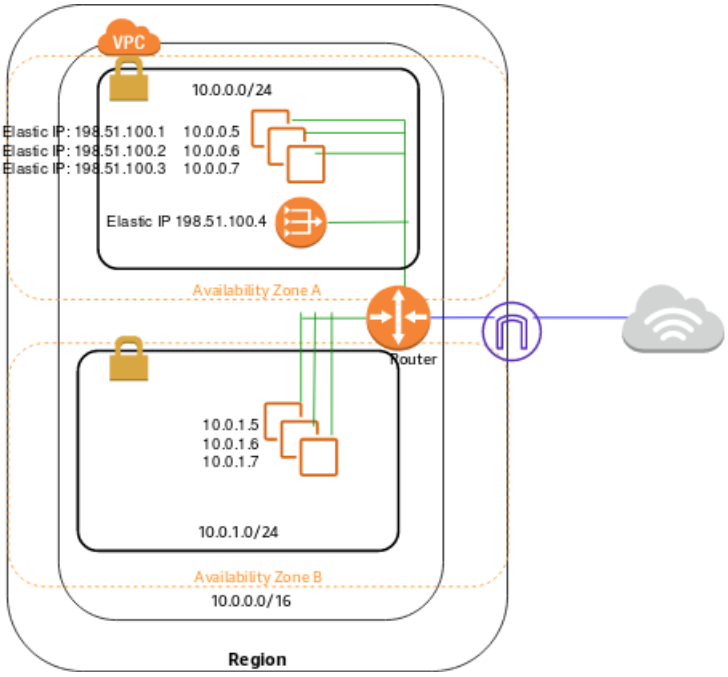
Todo gateway NAT é criado em uma Zona de disponibilidade específica e implementado com redundância nessa zona. Existe uma cota de gateways NAT que podem ser criados em uma zona de disponibilidade. Para obter mais informações, consulte Cotas da Amazon VPC (p. 345).

> **Note**
>
> 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 criar uma Zona de disponibilidade com arquitetura independente, 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.

Caso não precise mais de um gateway NAT, você pode excluí-lo. A exclusão de um gateway NAT dissocia o respectivo endereço IP elástico, mas não libera o endereço de sua conta.

O diagrama a seguir mostra a arquitetura desse de uma VPC com um gateway NAT. A tabela de rotas principal envia tráfego de internet das instâncias na sub-rede privada para o gateway NAT. O gateway NAT envia o tráfego para o gateway da internet usando o endereço IP elástico do gateway NAT como o endereço IP de origem.



Uma tabela de rota personalizada é associada à sub-rede na zona de disponibilidade A. A primeira entrada é padrão para o roteamento local na VPC; essa entrada permite que as instâncias na VPC comuniquem-se entre si. A segunda entrada envia todos os outros tráfegos da sub-rede ao gateway da Internet.

Destino	Destino
`10.0.0.0/16`	local
`0.0.0.0/0`	internet-gateway-id

A tabela de rotas principal está associada à sub-rede na zona de disponibilidade B. A primeira entrada é padrão para o roteamento local na VPC; essa entrada permite que as instâncias na VPC comuniquem-se entre si. A segunda entrada envia todos os outros tráfegos da sub-rede ao gateway NAT.

Destino	Destino
`10.0.0.0/16`	local
`0.0.0.0/0`	nat-gateway-id

Regras e limitações do gateway NAT

Um gateway NAT tem as características e limitações a seguir:

- Um gateway NAT comporta 5 Gbps de largura de banda e escala automaticamente até 45 Gbps. Se você precisar de mais, é possível distribuir a carga de trabalho dividindo os recursos em várias sub-redes e criando um gateway NAT em cada sub-rede.
- Você pode associar precisamente um endereço IP elástico ao gateway NAT. Não é possível dissociar um endereço IP elástico de um gateway NAT depois que ele é criado. Para usar outro endereço IP elástico no gateway NAT, crie um novo gateway NAT com o endereço necessário, atualize suas tabelas de rotas e, em seguida, exclua o gateway NAT existente, caso não precise mais dele.
- Um gateway NAT é compatível com os seguintes protocolos: TCP, UDP e ICMP.
- Não é possível associar um security group a um gateway NAT. Você pode usar security groups para suas instâncias em sub-redes privadas para controlar o tráfego para e proveniente dessas instâncias.
- Você pode usar uma Network ACL para controlar o tráfego para e proveniente da sub-rede na qual o gateway NAT está localizado. Uma Network ACL é aplicável ao tráfego do gateway NAT. Um gateway NAT usa as portas 1024 a 65535. Para obter mais informações, consulte Network ACLs (p. 190).
- No momento em que um gateway NAT é criado, ele recebe uma interface de rede à qual é automaticamente atribuído um endereço IP privado de um intervalo de endereços IP de sua 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.
- Mão é possível acessar o gateway NAT por uma conexão ClassicLink que esteja associada à sua VPC.
- Não é possível rotear o tráfego para um gateway NAT por meio de uma conexão de emparelhamento de VPC, uma conexão do Site-to-Site VPN ou do AWS Direct Connect. Um gateway NAT não pode ser usado por recursos que se encontram no outro lado dessas conexões.
- Um gateway NAT comporta no máximo 55.000 conexões simultâneas para cada destino exclusivo. Esse limite também se aplica se você criar aproximadamente 900 por segundo com um único destino (aproximadamente 55.000 conexões por minuto). Se o endereço IP de destino, a porta de destino ou o protocolo (TCP/UDP/ICMP) mudar, você poderá criar 55,000 conexões suplementares. Para mais de 55.000 conexões, há uma chance maior de erros de conexão devido a erros de alocação de porta. Esses erros podem ser monitorados visualizando a métrica do CloudWatch `ErrorPortAllocation` do gateway NAT. Para obter mais informações, consulte Monitorar gateways NAT usando o Amazon CloudWatch (p. 236).

Migrar de uma instância NAT

Se você já tiver uma instância NAT, poderá substituí-la por um gateway NAT. Para isso, crie um gateway NAT na mesma sub-rede de sua instância NAT e substitua a rota existente em sua tabela direcionada à instância NAT que tem uma rota para o gateway NAT. Para usar o mesmo endereço IP elástico para o gateway NAT que você usa atualmente 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.

> Note
>
> 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).

Prática recomendada ao enviar tráfego para o Amazon S3 ou o DynamoDB na mesma região

Para evitar cobranças por processamento de dados para gateways NAT ao acessar o Amazon S3 e o DynamoDB que estejam na mesma região, configure um endpoint de gateway e faça o roteamento do

tráfego por meio dele, em vez do gateway NAT. Não há cobranças pelo uso de um endpoint do gateway. Para obter mais informações, consulte VPC endpoints do gateway.

Trabalhar com gateways NAT

É possível usar o console da Amazon VPC para criar, visualizar e excluir um gateway NAT. Além disso, é possível usar o assistente da Amazon VPC para criar uma VPC com uma sub-rede pública, uma sub-rede privada e um gateway NAT. Para obter mais informações, consulte VPC com sub-redes públicas e privadas (NAT) (p. 31).

Tarefas

- Criar um gateway NAT (p. 232)
- Atualizar a tabela de rotas (p. 232)
- Excluir um gateway NAT (p. 233)
- Testar um gateway NAT (p. 233)

Criar um gateway NAT

Para criar um gateway NAT, é necessário especificar uma sub-rede e um endereço IP elástico. Verifique se no momento o endereço IP elástico está associado a uma instância ou a uma interface de rede. Se estiver migrando de uma instância NAT para um gateway NAT e desejar reutilizar o endereço IP elástico da instância NAT, deverá primeiro dissociar o endereço de sua instância NAT.

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 NAT Gateways, Create NAT Gateway.
3. Especifique a sub-rede na qual criará o gateway NAT e selecione o ID de alocação de um endereço IP elástico para associá-lo ao gateway NAT.
4. (Opcional) Adicione ou remova uma tag.

   [Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

   - Em Key (Chave), insira o nome da chave.
   - Em Value (Valor), insira o valor da chave.

   [Remover uma tag] Selecione o botão de exclusão ("x") à direita da chave e do valor da tag.
5. Escolha Create a NAT Gateway (Criar um gateway NAT).
6. O gateway NAT é exibido no console. Após alguns instantes, quando o status muda para `Available`, ele estará pronto para ser usado.

Se o gateway NAT adquirir o status `Failed`, isso significa que ocorreu um erro durante sua criação. Para obter mais informações, consulte Falha na criação do gateway NAT (p. 241).

Atualizar a tabela de rotas

Depois de criar o gateway NAT, você deve atualizar as tabelas de rotas de suas sub-redes privadas para apontarem o tráfego da internet para o gateway NAT. Para determinar como o tráfego deve ser roteado, usamos a rota mais específica que corresponde ao tráfego (correspondência de prefixo mais longa). Para obter mais informações, consulte Prioridade de rota (p. 290).

Para criar uma rota para um gateway NAT

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 associada à sua sub-rede privada e escolha Routes, Edit.
4. Escolha Add another route. Em Destination, insira `0.0.0.0/0`. Em Target, selecione o ID de seu gateway NAT.

   Note

   Se estiver migrando de uma instância NAT, poderá substituir a rota atual direcionada para uma instância NAT por uma rota para o gateway NAT.
5. Escolha Salvar.

Para garantir que seu gateway NAT possa acessar a internet, a tabela de rotas associada à sub-rede na qual seu gateway NAT reside deve conter uma rota que aponte o tráfego da internet para um gateway da internet. Para obter mais informações, consulte Criar uma tabela de rotas personalizada (p. 216). 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 obter mais informações, consulte Adicionar e remover rotas de uma tabela (p. 303).

Excluir um gateway NAT

É possível excluir um gateway NAT usando o console da Amazon VPC. 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.

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 gateway NAT e escolha Actions, Delete NAT Gateway.
4. Na caixa de diálogo de confirmação, escolha Delete NAT Gateway.
5. Se não for mais necessário o endereço IP elástico associado ao gateway NAT, recomendamos que você o libere. Para obter mais informações, consulte Liberar um endereço IP elástico (p. 281).

Testar um gateway NAT

Depois que criar o gateway NAT e atualizar as tabelas de rotas, você poderá executar ping em alguns 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 (p. 234).

Se não for possível conectar-se à internet, você também poderá executar os testes a seguir para determinar se o tráfego da internet está sendo roteado através do gateway NAT:

- Você pode rastrear 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 (normalmente, no 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 de seu gateway NAT. É possível obter o endereço IP elástico e o endereço IP privado do gateway NAT visualizando as respectivas informações na página NAT Gateways no console da Amazon VPC.

Se os testes anteriores falharem, consulte Solucionar problemas com gateways NAT (p. 241).

Testar a conexão com a Internet

O exemplo a seguir demonstra como testar se a instância em uma sub-rede privada pode conectar-se com a Internet.

1. Execute uma instância em sua sub-rede pública (você a usa como bastion host). Para obter mais informações, consulte Executar uma instância na sub-rede (p. 114). No assistente de execução, 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 assistente de execução, selecione uma Amazon Linux AMI. Não atribua um endereço IP público à sua instância. Confirme se as regras de seu security group 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 host bastion na sub-rede pública. Para obter mais informações, consulte Para configurar o encaminhamento de agente SSH para Linux ou macOS (p. 234) ou Para configurar o encaminhamento de agente SSH para Windows (PuTTY) (p. 234).
4. No host bastion, 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 (p. 235).

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
   ```

Para configurar o encaminhamento de agente SSH para 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 com PuTTYgen no Guia do usuário do Amazon EC2 para instâncias do Linux.
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. 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 (p. 244).

3. (Opcional) Se você não precisar mais das instâncias, encerre-as. Para obter mais informações, consulte Encerrar a instância no Guia do usuário do Amazon EC2 para instâncias do Linux.

Controlar o uso de gateways NAT

Por padrão, os usuários do IAM não têm permissão para trabalhar com gateways NAT. É possível criar uma política de usuário do IAM que conceda permissão aos usuários para criar, descrever e excluir gateways NAT. No momento, não oferecemos permissões de recurso para nenhuma `ec2:*NatGateway*` operação de API. Para obter mais informações sobre políticas do IAM para Amazon VPC, consulte Identity and Access Management para o Amazon VPC (p. 162).

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 recursos do Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias do Linux.

Há suporte a tags de alocação de custo para gateways NAT. Portanto, também é possível usar tags para organizar sua fatura da AWS e refletir sua própria estrutura de custo. Para mais informações, consulte Usar tags de alocação de custos no Guia do usuário do Gerenciamento de faturamento e custos da AWS. 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.

Visão geral da API e da CLI

Você pode executar as tarefas descritas nesta página usando a linha de comando ou uma API. Para obter mais informações sobre as interfaces de linha de comando e uma lista de operações de API disponíveis, consulte Acessar a Amazon VPC (p. 1).

Criar um gateway NAT

- create-nat-gateway (CLI da AWS)
- New-EC2NatGateway (AWS Tools for Windows PowerShell)
- CreateNatGateway (API de consulta do Amazon EC2)

Marcar um gateway NAT

- create-tags (CLI da AWS)
- New-EC2Tag (AWS Tools for Windows PowerShell)
- CreateTags (API de consulta do Amazon EC2)

Descrever um gateway NAT

- describe-nat-gateways (CLI da AWS)
- Get-EC2NatGateway (AWS Tools for Windows PowerShell)
- DescribeNatGateways (API de consulta do Amazon EC2)

Excluir um gateway NAT

- delete-nat-gateway (CLI da AWS)
- Remove-EC2NatGateway (AWS Tools for Windows PowerShell)
- DeleteNatGateway (API de consulta do Amazon EC2)

Monitorar gateways NAT usando 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. Os dados de métricas do gateway NAT são fornecidos em intervalos de um minuto, e as estatísticas são registradas durante um período de 15 meses.

Para obter mais informações sobre o Amazon CloudWatch, consulte o Guia do usuário do Amazon CloudWatch. Para obter mais informações sobre a definição de preço, consulte Definição de preço do Amazon CloudWatch.

Métricas e dimensões do gateway NAT

As métricas a seguir estão disponíveis para os gateways NAT.

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. Se o valor para `BytesOutToSource` for menor que o valor de `BytesInFromDestination`, talvez haja perda de dados durante o processamento de gateway NAT ou tráfego ativo bloqueado pelo gateway NAT.

Métrica	Descrição
	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`, pode 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`, pode haver perda de dados durante o processamento do gateway NAT. Unidade: bytes Statistics: a estatística mais útil é `Sum`.
`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 de gateway NAT ou tráfego ativo 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`.
`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 corretamente 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, pode ser que os clientes atrás do gateway NAT estejam reutilizando conexões obsoletas. Unidade: contagem Statistics: a estatística mais útil é `Sum`.
`PacketsDropCount`	O número de pacotes removidos pelo gateway NAT. Um valor maior que zero pode indicar um problema temporário contínuo com o gateway NAT. Se esse valor for alto, consulte o AWS service health dashboard. Unidades: contagem Statistics: a estatística mais útil é `Sum`.

Métrica	Descrição
`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 de gateway NAT ou tráfego ativo bloqueado pelo gateway NAT. Unidade: contagem Statistics: a estatística mais útil é `Sum`.
`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`, pode 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`, pode haver perda de dados durante o processamento do gateway NAT. Unidade: contagem Statistics: a estatística mais útil é `Sum`.
`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 de gateway NAT ou tráfego ativo bloqueado pelo gateway NAT. Unidade: contagem Statistics: a estatística mais útil é `Sum`.

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. Você pode visualizar as métricas dos gateways NAT da maneira a seguir.

Como exibir métricas usando o console do CloudWatch

As métricas são agrupadas primeiro pelo namespace do serviço e, em seguida, por várias combinações de dimensão dentro de cada namespace.

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Métricas.
3. Em All metrics, escolha o namespace de métrica NAT gateway.
4. Para visualizar as métricas, selecione a 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

É possível 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, Create Alarm.
3. Escolha NAT gateway.
4. Selecione o gateway NAT e a métrica BytesOutToDestination e escolha Next.
5. Configure o alarme como a seguir e escolha Create Alarm ao concluir:
   - Em Alarm Threshold, insira um nome e uma descrição para o alarme. Em Whenever, escolha >= e insira `5000000`. Insira 1 em períodos consecutivos.
   - Em Actions, selecione uma lista de notificações existente ou escolha New list para criar uma nova.
   - Em Alarm Preview, selecione um período de 15 minutos e especifique a estatística Sum.

Você pode cria um alarme que monitora a métrica `ErrorPortAllocation` e envia 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, Create Alarm.
3. Escolha NAT Gateway.
4. Selecione o gateway NAT e a métrica ErrorPortAllocation e escolha Next.
5. Configure o alarme como a seguir e escolha Create Alarm ao concluir:
   - Em Alarm Threshold, insira um nome e uma descrição para o alarme. Em Whenever, escolha > e insira `0`. Insira 3 em períodos consecutivos.
   - Em Actions, selecione uma lista de notificações existente ou escolha New list para criar uma nova.
   - Em Alarm Preview, selecione um período de 5 minutos e especifique a estatística Maximum.

Para obter mais exemplos de como criar alarmes, consulte Criar alarmes do Amazon CloudWatch no Guia do usuário do Amazon CloudWatch.

Solucionar problemas com 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

Problema

Você cria um gateway NAT e ele entra no status `Failed`.

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, acesse o console da Amazon VPC e selecione NAT Gateways (Gateways NAT). Selecione o gateway NAT e visualize a mensagem de erro no campo Status message (Mensagem de status) no painel de 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.

Note

O gateway NAT com falha será excluído automaticamente após um breve período (normalmente em cerca de uma hora).

Erro exibido	Causa	Solução
Subnet has insufficient free addresses to create this NAT gateway	A sub-rede que você especificou 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 interfaces de rede não usadas ou 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 associe um gateway da internet à VPC. Para obter mais informações, consulte Criar e associar de um gateway da Internet (p. 215).
Elastic IP address eipalloc-xxxxxxxx could not be associated with this NAT gateway	O endereço IP elástico que você especificou não existe ou não foi possível encontrá-lo.	Examine o ID de alocação do endereço IP elástico para ver se você a inseriu corretamente. Verifique se você especificou um endereço IP elástico que está na mesma região da AWS em que está criando o gateway NAT.
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 especificados 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 obter mais informações, consulte Trabalhar com endereços IP elásticos (p. 278).
Network interface eni-xxxxxxxx, created and used internally by	Houve um problema ao criar ou usar a interface de rede do gateway NAT.	Não é possível resolver este erro. Tente criar um gateway NAT novamente.

Erro exibido	Causa	Solução
this NAT gateway is in an invalid state. Tente novamente.		

Endereço IP elástico e cotas do gateway NAT

Problema

Ao tentar alocar um endereço IP elástico, você obtém o erro a seguir.

```
The maximum number of addresses has been reached.
```

Ao tentar criar um gateway NAT, você obtém o erro a seguir.

```
Performing this operation would exceed the limit of 5 NAT gateways
```

Causa

Há duas causas possíveis:

- Você atingiu a cota do número de endereços IP elásticos para sua conta para essa Região.
- Você atingiu a cota do número de gateways NAT para sua conta para essa zona de disponibilidade.

Solução

Se tiver atingido a cota de endereços IP elásticos, você poderá desassociar um endereço IP elástico de outro recurso. Como alternativa, é possível solicitar um aumento de cota usando o Formulário de limites da Amazon VPC.

Se tiver atingido a cota de seu gateway NAT, você poderá usar uma das seguintes opções:

- Solicite um aumento de cota usando o Formulário de limites da Amazon VPC. A cota do gateway NAT é aplicada por zona de disponibilidade.
- 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 (p. 345).

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 outra Zona de disponibilidade 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

Talvez tenha havido um erro ao criar o gateway NAT e ele falhou. Um gateway NAT com um status `Failed` fica visível no console da Amazon VPC por um breve período (normalmente, uma hora). Após uma hora, ele é excluído automaticamente.

Solução

Examine as informações em Falha na criação do gateway NAT (p. 241) 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 um gateway NAT (p. 233).

As instâncias não conseguem acessar a Internet

Problema

Você criou um gateway NAT 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 (p. 241).
- 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. Para obter mais informações, consulte Criar uma tabela de rotas personalizada (p. 216).
  - A instância deve estar em uma sub-rede privada com uma tabela de rotas que roteia o tráfego da internet para o gateway NAT. Para obter mais informações, consulte Atualizar a tabela de rotas (p. 232).
  - 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.

  Note

  O gateway NAT propriamente dite permite tráfego de saída e tráfego recebido em resposta a uma solicitação de saída (por isso, ele é stateful).
- 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.

  Note

  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 VPC Flow Logs (p. 310).
- Se estiver usando o comando `ping`, verifique se está executando ping em um site 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. No momento, um gateway NAT não oferece suporte à fragmentação de IP para TCP nem para ICMP. Para obter mais informações, consulte Comparação entre gateways NAT e instâncias NAT (p. 255).
- 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.

   Note

   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 é possível estabelecer mais conexões.

Causa

Talvez você tenha atingido o limite de conexões simultâneas para um único gateway NAT. Para obter mais informações, consulte Regras e limitações do gateway NAT (p. 231). Se as instâncias na sub-rede privada criarem um grande número de conexões, você poderá atingir esse limite.

Solução

Faça uma das coisas a seguir:

- 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` (p. 236) no CloudWatch para monitorar aumentos nas conexões ociosas. Fechar as conexões ociosas para liberar capacidade.

Instâncias NAT

> **Important**
>
> O AMI NAT é construído com base na última versão do Amazon Linux, 2018.03, que chegou ao fim do suporte padrão em 31 de dezembro de 2020. Para obter mais informações, consulte a seguinte postagem no blog: Fim da vida útil do Amazon Linux AMI. Esse recurso só receberá atualizações críticas de segurança (não haverá atualizações regulares).
> Se você usar uma AMI NAT existente, a AWS recomenda migrar para um gateway NAT ou criar sua própria AMI NAT no Amazon Linux 2 o mais rápido possível. Para obter informações sobre como migrar sua instância, consulte the section called “Migrar de uma instância NAT” (p. 231).

É possível criar sua própria AMI de conversão de endereços de rede e executá-la em uma instância do EC2 como instância NAT em uma sub-rede pública na VPC para permitir que as instâncias na sub-rede privada iniciem tráfego IPv4 de saída para a Internet ou outros serviços da AWS, mas impedir que elas recebam tráfego de saída iniciado por alguém na Internet.

Para obter mais informações sobre sub-redes públicas e privadas, consulte Roteamento de sub-rede (p. 108). Para obter mais informações sobre NAT, consulte Dispositivos NAT para sua VPC (p. 228).

NAT não é compatível com tráfego IPv6, use um gateway da Internet apenas de saída em vez disso. Para obter mais informações, consulte Gateways da Internet apenas de saída (p. 218).

Sua cota de instância NAT depende da cota de instância para a região. Para obter mais informações, consulte Perguntas frequentes sobre o EC2.

> **Note**
>
> Além disso, você pode usar um gateway NAT, que consiste e um serviço NAT gerenciado que oferece maior disponibilidade e maior largura de banda e requer menor empenho administrativo. Para casos de uso comuns, é recomendável usar um gateway NAT, em vez de uma instância NAT. Para obter mais informações, consulte Gateways NAT (p. 229) e Comparação entre gateways NAT e instâncias NAT (p. 255).

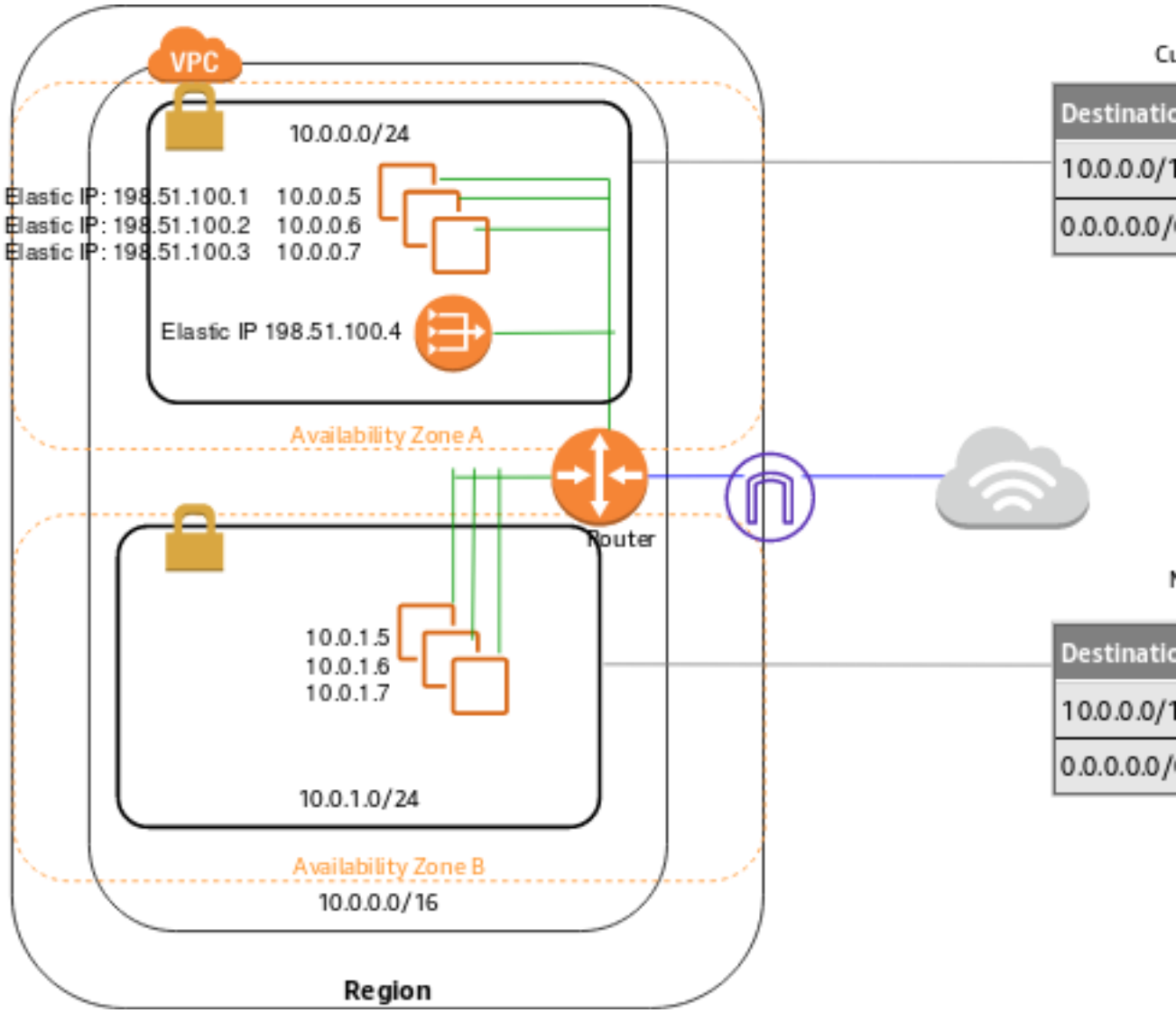
Tópicos

Noções básicas sobre a instância NAT

A figura a seguir mostra noções básicas sobre instância NAT. A tabela de rotas principal está associada à sub-rede privada e envia tráfego das instâncias na sub-rede privada à instância NAT na sub-rede pública. Depois, a instância NAT envia tráfego ao gateway da Internet para a VPC. O tráfego é atribuído ao endereço IP elástico 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.

O tráfego da Internet das instâncias na sub-rede privada é roteado para a instância NAT, que, por sua vez, se comunica com a Internet. Portanto, a instância NAT deve ter acesso à Internet. Ela deve estar em uma

sub-rede pública (uma sub-rede que tenha uma tabela de rotas com uma rota para o gateway da Internet) e deve ter um endereço IP público ou um endereço IP elástico.



AMI da instância NAT

Embora a Amazon forneça AMIs do Amazon Linux configuradas para serem executadas como instâncias NAT, elas são criadas com base na última versão do Amazon Linux, 2018.03, que chegou ao fim do suporte padrão em 31 de dezembro de 2020 e só receberá atualizações críticas de segurança (não haverá atualizações regulares). Se você usar uma AMI NAT existente (essas AMIs contêm a string `amzn-ami-vpc-nat` em seus nomes), a AWS recomenda migrar para um gateway NAT ou criar sua própria AMI NAT no Amazon Linux 2 o mais rápido possível.

Criar sua AMI NAT

Você pode começar com uma AMI do Amazon existente e fazer as devidas personalizações para criar sua própria AMI para ser executada como uma instância NAT. Você pode usar essa AMI na próxima vez em que precisar executar uma instância NAT. Recomendamos que você use a AMI mais recente do Amazon Linux 2 para criar sua própria AMI NAT. Para obter informações sobre como criar a AMI, consulte Criar AMIs baseadas em Amazon EBS no Guia do usuário do Amazon EC2 para instâncias do Linux.

Atualizar sua instância NAT existente

Se você já usa uma AMI NAT, recomendamos migrar para o NAT Gateway ou criar sua própria AMI NAT no Amazon Linux 2.

Configurar a instância NAT

Antes de começar, crie uma AMI configurada para ser executada como uma instância NAT. Para obter mais informações, consulte the section called “Criar sua AMI NAT” (p. 249). Essa AMI é exibida no painel de navegação do Console do Amazon Elastic Compute Cloud, em Images (Imagens) quando você filtra por Owned by me (De minha propriedade).

Para configurar a VPC e a instância NAT usando o console, siga estas etapas:

1. Crie uma VPC com duas sub-redes.
    a. Crie uma VPC (consulte Criar uma VPC (p. 110))
    b. Crie duas sub-redes (consulte Criar uma sub-rede (p. 215))
    c. Anexar um gateway da Internet à VPC (consulte Criar e associar de um gateway da Internet (p. 215))
    d. Crie uma tabela de rotas personalizada que envie o tráfego de saída da VPC ao gateway da Internet e depois a associe a uma sub-rede, tornando-a uma sub-rede pública (consulte Criar uma tabela de rotas personalizada (p. 216))
2. Crie um security group NATSG (consulte Criar um grupo de segurança NATSG (p. 251)). Você especificará esse security group ao executar a instância NAT.
3. Execute uma instância dentro da sua sub-rede pública de uma AMI configurada para ser executada como uma instância NAT.
    a. Abra o console do Amazon EC2.
    b. No painel, escolha o botão Launch Instance (Executar instância) e conclua o assistente como se segue:
        i. Na página Choose an Amazon Machine Image (AMI) (Selecione uma imagem de máquina da Amazon (AMI)), defina o filtro como Owned by me (De minha propriedade) e selecione sua AMI.
        ii. Na página Choose an Instance Type, selecione o tipo de instância e escolha Next: Configure Instance Details.
        iii. Na página Configure Instance Details, selecione a VPC que você criou na lista Network e selecione sua sub-rede pública na lista Subnet.
        iv. (Opcional) Marque a caixa de seleção Public IP para solicitar que sua instância NAT receba um endereço IP público. Se preferir não atribuir um endereço IP público no momento, poderá alocar um endereço IP elástico e atribuí-lo à sua instância depois que ela for executada. Para obter mais informações sobre como atribuir um IP público na execução, consulte Atribuir um endereço IPv4 público durante a execução da instância (p. 122). Escolha Next: Add Storage.
        v. Você pode optar por adicionar armazenamento à sua instância e na página seguinte pode adicionar tags. Escolha Next: Configure Security Group ao concluir.
        vi. Na página Configure Security Group, selecione a opção Select an existing security group e depois o security group NATSG que você criou. Escolha Review and Launch.
        vii. Revise as configurações que você escolheu. Faça qualquer alteração necessária e selecione Launch (Executar) para escolher um par de chaves e executar sua instância.
4. Desative o atributo `SrcDestCheck` da instância NAT (consulte Desativar as verificações de origem/destino (p. 252))
5. Se não atribuir um endereço IP público à instância NAT durante a execução (etapa 3), precisará associar a ela um endereço IP elástico.

a. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
b. No painel de navegação, escolha Elastic IPs e Allocate new address.
c. Escolha Allocate.
d. Selecione o endereço IP elástico na lista e escolha Actions, Associate address.
e. Selecione o recurso da interface de rede e a interface de rede para a instância NAT. Selecione o endereço para associar com o endereço IP elástico na lista Private IP e escolha Associate.

6. Atualize a tabela de rotas principal para enviar tráfego para a instância NAT. Para obter mais informações, consulte Atualizar a tabela de rotas principal (p. 253).

Executar uma instância NAT com a linha de comando

Para executar uma instância NAT na sub-rede, use um dos seguintes comandos: Para obter mais informações, consulte Acessar a Amazon VPC (p. 1). Você pode usar o ID de AMI da AMI configurada para executar como uma instância NAT. Para obter informações sobre como criar uma AMI no Amazon Linux 2, consulte Criar AMIs baseadas em Amazon EBS no Guia do usuário do Amazon EC2 para instâncias do Linux.

- run-instances (CLI da AWS)
- New-EC2Instance (AWS Tools for Windows PowerShell)

Criar um grupo de segurança NATSG

Defina o grupo de segurança NATSG tal como descrito na tabela a seguir para permitir que sua instância NAT receba tráfego vinculado à Internet de instâncias em uma sub-rede privada, bem como tráfego SSH proveniente 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.

NATSG: regras recomendadas

`Inbound`			
`Source`	`Protocol`	`Port range`	`Comments`
`10.0.1.0/24`	TCP	80	Permite tráfego HTTP de entrada de servidores na sub-rede privada.
`10.0.1.0/24`	TCP	443	Permite tráfego HTTPS de entrada de servidores na sub-rede privada.
Intervalo de endereços IP públicos da sua rede doméstica	TCP	22	Permite acesso SSH de entrada de sua rede doméstica à instância NAT (por meio do gateway da Internet).
`Outbound`			
`Destination`	`Protocol`	`Port range`	`Comments`
`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.

Para criar um security group NATSG

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Security Groups (Grupos de segurança), Create Security Group (Criar grupo de segurança).
3. Na caixa de diálogo Create Security Group, especifique `NATSG` como nome do security group e forneça uma descrição. Selecione o ID de sua VPC na lista VPC e escolha Yes, Create.
4. Selecione o security group NATSG que você acabou de criar. O painel de detalhes exibe informações sobre security group, bem como guias para trabalhar com as respectivas regras de entrada e saída.
5. Adicione regras de tráfego de entrada usando a guia Inbound Rules da seguinte forma:
   a. Selecione Edit.
   b. Escolha Add another rule e selecione HTTP na lista Type. No campo Source, especifique o intervalo de endereços IP de sua sub-rede privada.
   c. Escolha Add another rule e selecione HTTPS na lista Type. No campo Source, especifique o intervalo de endereços IP de sua sub-rede privada.
   d. Escolha Add another rule e selecione SSH na lista Type. No campo Source, especifique o intervalo de endereços IP públicos de sua rede.
   e. Escolha Salvar.
6. Adicione regras de tráfego de saída usando a guia Outbound Rules da seguinte forma:
   a. Selecione Edit.
   b. Escolha Add another rule e selecione HTTP na lista Type. No campo Destination, especifique `0.0.0.0/0`
   c. Escolha Add another rule e selecione HTTPS na lista Type. No campo Destination, especifique `0.0.0.0/0`
   d. Escolha Salvar.

Para obter mais informações, consulte Grupos de segurança para a VPC (p. 180).

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.

Você pode desativar o atributo `SrcDestCheck` para a instância NAT em execução ou encerrada usando o console ou a linha de comando.

Para desativar a verificação de origem/destino usando o 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 a instância NAT e escolha Actions (Ações) e depois Networking (Rede) e Change Source/Dest (Alterar origem/destino).
4. Verifique se a verificação de origem/destino está interrompida. Caso contrário, selecione Stop (Interromper).
5. Escolha Save (Salvar).

6. 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).

Para desativar a verificação de origem/destino usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações, consulte Acessar a Amazon VPC (p. 1).

- modify-instance-attribute (CLI da AWS)
- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Atualizar a tabela de rotas principal

Como a sub-rede privada em sua VPC não está associada a uma tabela de rotas personalizada, ela usa a tabela de rotas principal. Por padrão, a tabela de rotas principal permite que as instâncias em sua VPC comuniquem-se entre si. É necessário adicionar uma rota que envia todos os outros tráfegos da sub-rede à instância NAT.

Para atualizar a 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.
3. Selecione a tabela de rotas principal de sua VPC (a coluna Main exibe Yes). O painel de detalhes exibe as guias para trabalhar com as respectivas rotas, associações e propagação de rotas.
4. Na guia Routes, escolha Edit, especifique `0.0.0.0/0` na caixa Destination, selecione o ID da instância NAT na lista Target e escolha Save.
5. Na guia Subnet Associations (Associações de sub-rede), escolha Edit (Editar) e marque a caixa de seleção Associate (Associar) para a sub-rede privada. Escolha Salvar.

Para obter mais informações, consulte Tabelas de rotas para sua VPC (p. 283).

Testar a configuração da instância NAT

Assim que 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 usando a instância NAT como servidor Bastion. Para isso, atualize as regras de grupo de segurança da instância NAT para permitir tráfego ICMP de entrada e saída e permitir tráfego SSH de saída, execute a instância em sua sub-rede privada, configure o encaminhamento de agente SSH para acessar as instâncias em sua sub-rede privada, conecte-se à sua instância e teste a conectividade com a Internet.

Para atualizar o security group de sua instância NAT

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
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. Selecione Edit inbound rules (Editar regras de entrada) na guia Inbound rules (Regras de entrada).
5. Escolha Add rule (Adicionar regra). Escolha All ICMP - IPv4 (Todos ICMP - IPv4) para Type (Tipo). Escolha Custom (Personalizado) para Source (Fonte) e insira o intervalo de endereços IP da sua sub-rede privada (por exemplo, `10.0.1.0/24`). Selecione Save rules (Salvar regras).
6. Escolha Edit outbound rules (Editar regras de saída) na guia Outbound rules (Regras de saída).

7. Escolha Add rule (Adicionar regra). Escolha SSH para Type (Tipo) . Escolha Custom (Personalizado) para Destination (Destino) e insira o intervalo de endereços IP da sua sub-rede privada (por exemplo, `10.0.1.0/24`).
8. Escolha Add rule (Adicionar regra). Escolha All ICMP - IPv4 (Todos ICMP - IPv4) para Type (Tipo). Escolha Custom (Personalizado) para Destination (Destino) e digite `0.0.0.0/0`. Selecione Save rules (Salvar regras).

Para executar uma instância em sua sub-rede privada

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Execute uma instância em sua sub-rede privada. Para obter mais informações, consulte Executar uma instância na sub-rede (p. 114). Lembre-se de configurar as opções a seguir no assistente de execução e escolha Launch:
   - Na página Choose an Amazon Machine Image (AMI), selecione Amazon Linux AMI na categoria Quick Start.
   - Na página Configure Instance Details, selecione sua sub-rede privada na lista Subnet e não atribua um endereço IP público à sua instância.
   - Na página Configure Security Group, seu security group deve incluir uma regra de entrada que permita acesso SSH do endereço IP privado de sua instância NAT ou do intervalo de endereços IP de sua sub-rede pública e deve haver uma regra de saída que permita tráfego ICMP de saída.
   - Na caixa de diálogo Select an existing key pair or create a new key pair, selecione o mesmo par de chaves usado para executar a instância NAT.

Para configurar o encaminhamento de agente SSH para Linux ou OS X

1. Em seu computador local, adicione sua chave privada para o agente de autenticação.

   Para o Linux, use o comando a seguir:

   ```
   ssh-add -c mykeypair.pem
   ```

   Para o OS X, use o comando a seguir:

   ```
   ssh-add -K mykeypair.pem
   ```

2. Conecte-se à sua instância NAT usando a opção `-A` para permitir encaminhamento de agente SSH; por exemplo:

   ```
   ssh -A ec2-user@54.0.0.123
   ```

Para configurar o encaminhamento de agente SSH para 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 com PuTTYgen.
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, insira a senha se necessário e escolha Open.
4. Inicie uma seção PuTTY para se conectar à sua instância NAT. Na categoria Auth, selecione a opção Allow agent forwarding e deixe o campo Private key file for authentication vazio.

Para testar a conexão com a internet

1. Teste se sua instância NAT consegue se comunicar com a Internet executando o comando `ping` para um site habilitado para ICMP; por exemplo:

```
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=48 time=74.9 ms
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=2 ttl=48 time=75.1 ms
...
```

   Pressione Ctrl+C no teclado para cancelar o comando `ping`.
2. Em sua instância NAT, conecte-se à sua instância na sub-rede privada usando o respectivo endereço IP privado; por exemplo:

```
ssh ec2-user@10.0.1.123
```

3. Em sua instância privada, teste se você consegue se conectar à Internet executando o comando `ping`:

```
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, verifique as seguintes informações:

   - Verifique se as regras de security group de sua instância NAT permitem tráfego ICMP de entrada de sua sub-rede privada. Se não, sua instância NAT não conseguirá receber o comando `ping` de sua instância privada.
   - Verifique se você configurou corretamente as tabelas de rotas. Para obter mais informações, consulte Atualizar a tabela de rotas principal (p. 253).
   - Lembre-se de desativar a verificação de origem/destino para sua instância NAT. Para obter mais informações, consulte Desativar as verificações de origem/destino (p. 252).
   - Lembre-se também de que você deve executar ping em um site habilitado para ICMP. Se não, você não receberá pacotes de resposta. Para testar, execute o mesmo comando `ping` no terminal de linha de comando de seu computador.
4. (Opcional) Encerre sua instância privada se não precisar mais dela. Para obter mais informações, consulte Encerrar a instância no Guia do usuário do Amazon EC2 para instâncias do Linux.

Comparação entre gateways NAT e instâncias NAT

A seguir se encontra um resumo detalhado das diferenças entre instâncias NAT e gateways NAT.

Atributo	gateway NAT	Instância do NAT
Disponibilidade	Altamente disponível. Em cada Zona de disponibilidade são implementados gateways	Use um script para gerenciar o failover entre as instâncias.

Atributo	gateway NAT	Instância do NAT
	NAT com redundância. Crie um gateway NAT em cada Zona de disponibilidade para assegurar uma arquitetura independente de zona.	
Largura de banda	Pode escalar até 45 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.
Desempenho	O software é otimizado por meio do gerenciamento do tráfego NAT.	Uma Amazon Linux AMI genérica que é configurada para executar 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.
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 carga de trabalho.
Endereços IP públicos	Escolha o endereço IP elástico para associar a um gateway NAT no momento de criá-lo.	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 pode ser associado a um gateway NAT. Você pode associar security groups aos seus recursos subjacentes ao 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.
Servidores bastion	Não compatível.	Use um servidores bastion.
Métricas de tráfego	Veja as métricas do CloudWatch para o gateway NAT (p. 236).	Visualize as métricas do CloudWatch para a instância.

Atributo	gateway NAT	Instância do NAT
Comportamento do tempo limite	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).	Quando uma conexão atinge o tempo limite, uma instância NAT envia um pacote FIN a qualquer recurso subjacente 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.

Conjuntos de opções de DHCP

O DHCP (Dynamic Host Configuration Protocol) fornece um padrão para transmitir informações de configuração aos hosts em uma rede TCP/IP. O campo `options` de uma mensagem DHCP contém parâmetros de configuração, incluindo o nome de domínio, o servidor de nomes de domínio e o netbios-node-type.

Quando você cria uma VPC, criamos automaticamente um conjunto de opções DHCP e as associamos a VPC. Você pode configurar suas próprias opções de DHCP definidas para a VPC.

Tópicos

Visão geral dos conjuntos de opções DHCP

Por padrão, todas as instâncias em uma VPC não padrão recebem um nome de host não resolvido que a AWS atribui (por exemplo, ip-10-0-0-202). Você pode atribuir seu próprio nome de domínio às suas instâncias e usar até quatro de seus próprios servidores DNS. Para fazer isso, você deve especificar um conjunto especial de opções DHCP para usar com a VPC.

A seguir estão as opções compatíveis para um conjunto de opções DHCP e o valor fornecido nas opções padrão DHCP definidas para a VPC. É possível especificar apenas as opções necessárias no seu conjunto de opções DHCP. Para obter mais informações sobre as opções, consulte RFC 2132.

domain-name-servers

Os endereços IP de até quatro servidores de nome de domínio ou o AmazonProvidedDNS (p. 258). Se estiver especificando mais de um servidor de nomes de domínio, separe-os com vírgulas. Embora você possa especificar até quatro servidores de nomes de domínio, observe que alguns sistemas operacionais podem impor limites inferiores.

Para usar essa opção, defina-a como AmazonProvidedDNS ou servidores de nomes de domínio personalizados. Se você definir essa opção como ambos, o resultado poderá causar um comportamento inesperado.

Conjunto de opções padrão DHCP: AmazonProvidedDNS

domain-name

O nome de domínio para as instâncias. Você pode especificar um nome de domínio personalizado (por exemplo, `example.com`). Este valor é usado para completar nomes de host DNS não qualificados. Para obter mais informações sobre os nomes de host do DNS e suporte a DNS na VPC, consulte Usar DNS com a VPC (p. 262) Ao usar um nome de domínio personalizado, você só precisará especificar um servidor de nome de domínio personalizado se ele estiver hospedado em servidores DNS gerenciados pelo cliente. Se você usa a zona hospedada privada do Amazon Route 53 associada à mesma VPC, pode usar o AmazonProvidedDNS (p. 258).

Important

Alguns sistemas operacionais Linux aceitam vários nomes de domínio separados por espaços. No entanto, outros sistemas operacionais Linux e Windows 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 tenha instâncias com vários sistemas operacionais, especifique apenas um nome de domínio.

Opções padrão DHCP definidas: para `us-east-1`, o valor é `ec2.internal`. Para outras Regiões, o valor é *`region`*.compute.internal (por exemplo, `ap-northeast-1.compute.internal`). Para usar os valores padrão, defina `domain-name-servers` para o AmazonProvidedDNS.

ntp-servers

Os endereços IP de até quatro servidores NTP (Network Time Protocol). Para obter mais informações, consulte a seção 8.3 do RFC 2132. Você pode especificar o Amazon Time Sync Service em `169.254.169.123`. Para obter mais informações, consulte Definir o horário no Guia do usuário do Amazon EC2 para instâncias do Linux.

Opções padrão DHCP definidas: nenhuma

netbios-name-servers

Os endereços IP de até quatro servidores de nomes NetBIOS.

Opções padrão DHCP definidas: nenhuma

netbios-node-type

O tipo de nó NetBIOS (1, 2, 4 ou 8). Recomendamos que você especifique 2 (ponto a ponto ou P-nó). 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.

Opções padrão DHCP definidas: nenhuma

Servidor DNS da Amazon

As opções padrão de DHCP definidas para a VPC incluem duas opções: `domain-name-servers=AmazonProvidedDNS`e *`domain-name-for-your-region`*`domain-name=`. AmazonProvidedDNS é um servidor do Amazon Route 53 Resolver, e esta opção habilita o DNS para instâncias que precisam se comunicar por meio do gateway da Internet da VPC. A string `AmazonProvidedDNS` mapeia para um servidor DNS executado em um endereço IP reservado na base do intervalo de rede IPv4 da VPC, mais dois. Por exemplo, o servidor DNS em uma rede 10.0.0.0/16 está localizado em 10.0.0.2. Para VPCs com vários blocos CIDR IPv4, o endereço IP do servidor DNS está localizado no bloco CIDR principal. O servidor DNS não reside em uma sub-rede ou zona de disponibilidade específica em uma VPC.

Quando você executa uma instância em uma VPC, fornecemos a instância um nome de host DNS privado e um nome de host DNS público se a instância recebe um endereço público IPv4. Se `domain-name-servers` estiverem configurados como AmazonProvidedDNS nas opções DHCP, o nome de host DNS público adquirirá o formato `ec2-`*`public-ipv4-address`*`.compute-1.amazonaws.com` para a região

us-east-1 e `ec2-public-ipv4-address.region.compute.amazonaws.com` para outras regiões. O nome do host privado adquire a forma `ip-private-ipv4-address.ec2.internal` para a região us-east-1 e `ip-private-ipv4-address.region.compute.internal` para outras regiões. Para alterá-los para nomes de host DNS personalizados, você deve configurar `domain-name-servers` para um servidor DNS personalizado.

O servidor DNS da Amazon na VPC é usado para resolver 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 DNS da Amazon, as seguintes regras e considerações se aplicam.

- Não é possível filtrar o tráfego de ou para um servidor DNS da Amazon usando network ACLs ou grupos de segurança.
- Os serviços que utilizam a estrutura de trabalho Hadoop, como o Amazon EMR, requerem instâncias para resolver 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 DNS para encaminhar consultas para o domínio *region-name*`.compute.internal` para o servidor DNS da Amazon. Para obter mais informações, consulte Configurar uma VPC para hospedar clusters no Guia de gerenciamento do Amazon EMR.
- Você pode usar o endereço IP do servidor DNS da Amazon 169.254.169.253, embora alguns servidores não permitam seu uso. O Windows Server 2008, por exemplo, não permite o uso de um servidor DNS localizado no intervalo de rede 169.254.x.x.
- O Amazon Route 53 Resolver é compatível apenas com consultas DNS recursivas.

Alterar opções DHCP

Depois de criar um conjunto de opções DHCP, você não pode modificá-las. Se você quiser que sua VPC use um conjunto diferente de opções DHCP, será necessário criar um novo conjunto e associá-lo a sua VPC. Você também pode configurar sua VPC para não usar nenhuma opção DHCP.

Você pode ter vários conjuntos de opções DHCP, mas você pode associar apenas um conjunto de opções DHCP a uma VPC por vez. Se você excluir uma VPC, o conjunto de opções DHCP associado à VPC será desassociado dela.

Depois de associar um novo conjunto de opções DHCP a uma VPC, todas as instâncias existentes e todas as novas instâncias que você inicia na VPC usarão as novas opções. Você não precisa reiniciar ou executar novamente as instâncias. Eles automaticamente recuperam as mudanças dentro de algumas horas, dependendo da frequência com que a instância renova sua concessão DHCP. Se você quiser, é possível renovar explicitamente a concessão usando o sistema operacional na instância.

Trabalhar com conjuntos de opções DHCP

Esta seção mostra como trabalhar com conjuntos de opções DHCP.

Tarefas

- Criar um conjunto de opções DHCP (p. 260)
- Alterar o conjunto de opções DHCP utilizado por uma VPC (p. 260)
- Alterar uma VPC para não usar opções DHCP (p. 261)
- Modificar as tags de um conjunto de opções DHCP (p. 261)
- Excluir um conjunto de opções DHCP (p. 261)

Criar um conjunto de opções DHCP

Você pode criar tantos conjuntos de opções DHCP adicionais quanto quiser. No entanto, você só pode associar uma VPC a um conjunto de opções DHCP por vez. Depois de criar um conjunto de opções DHCP, você deve configurar sua VPC para usá-la. Para obter mais informações, consulte Alterar o conjunto de opções DHCP utilizado por uma VPC (p. 260).

Para criar um conjunto de opções DHCP

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha DHCP Options Sets.
3. Na caixa de diálogo, insira valores para as opções que deseja usar.

   Important

   Se a VPC tiver um gateway da Internet, certifique-se de especificar seu próprio servidor DNS ou o servidor DNS da Amazon (AmazonProvidedDNS) para o valor Domain name servers (Servidores de nomes de domínio). Caso contrário, as instâncias que precisam se comunicar com a Internet não terão acesso ao DNS.
4. Opcionalmente, adicione ou remova uma tag.

   [Adicionar uma tag] Escolha Adicionar nova tag e faça o seguinte:

   - Em Key (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. Escolha Create DHCP Options set.

   O novo conjunto de opções DHCP aparece na sua lista de opções DHCP.
6. Anote o ID do novo conjunto de opções DHCP (dopt-xxxxxxxx). Você precisará desse ID para associar o novo conjunto de opções à VPC.

Agora que você criou um conjunto de opções DHCP, será necessário associá-lo à VPC para que as opções tenham efeito. Você pode criar vários conjuntos de opções DHCP, mas é possível associar apenas um conjunto de opções DHCP a sua VPC ao mesmo tempo.

Alterar o conjunto de opções DHCP utilizado por uma VPC

Você pode alterar qual o conjunto de opções DHCP que sua VPC usa. Se desejar que as configurações da VPC não usem opções DHCP, consulte Alterar uma VPC para não usar opções DHCP (p. 261).

Note

O procedimento a seguir pressupõe que você já criou o conjunto de opções DHCP para o qual deseja alterar. Caso contrário, crie o conjunto de opções agora. Para obter mais informações, consulte Criar um conjunto de opções DHCP (p. 260).

Para alterar o conjunto de opções DHCP associado 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 e Actions, Edit DHCP options set (Ações, editar conjunto de opções DHCP).
4. Na lista DHCP options set (Conjunto de opções DHCP), selecione um conjunto de opções na lista e selecione Save (Salvar).

Depois de associar um novo conjunto de opções DHCP à VPC, todas as instâncias existentes e todas as novas instâncias iniciadas nessa VPC usarão as novas opções. Você não precisa reiniciar ou executar novamente as instâncias. Eles automaticamente recuperam as mudanças dentro de algumas horas, dependendo da frequência com que a instância renova sua concessão DHCP. Se você quiser, é possível renovar explicitamente a concessão usando o sistema operacional na instância.

Alterar uma VPC para não usar opções DHCP

É possível configurar a VPC para que ela não use um conjunto de opções DHCP.

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 Actions, Edit DHCP options set (Ações, editar conjunto de opções DHCP).
4. Na lista DHCP options set (Conjunto de opções DHCP), selecione No DHCP options set (Nenhum conjunto de opções DHCP) na lista e selecione Save (Salvar).

Você não precisa reiniciar ou executar novamente as instâncias. Eles automaticamente recuperam as mudanças dentro de algumas horas, dependendo da frequência com que a instância renova sua concessão DHCP. Se você quiser, é possível renovar explicitamente a concessão usando o sistema operacional na instância.

Modificar as tags de um conjunto de opções DHCP

É possível adicionar tags para identificar facilmente o conjunto de opções. Adicione uma tag ao conjunto de opções DHCP ou remova uma tag do conjunto de opções DHCP.

Como modificar as tags de um conjunto de opções DHCP

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha DHCP options sets (Conjuntos de opções DHCP).
3. Selecione o conjunto de opções DHCP e selecione Actions, Manage tags (Ações, gerenciar tags).
4. Adicione ou remova uma tag.

   [Adicionar uma tag] Escolha Add new tag (Adicionar nova tag) e faça o seguinte:
   - Em Key (Chave), insira o nome da chave.
   - Em Value (Valor), insira o valor da chave.

   [Remover uma tag] Ao lado da tag, escolha Remove (Remover).
5. Escolha Save (Salvar).

Excluir um conjunto de opções DHCP

Quando você não precisa mais de um conjunto de opções DHCP, use o procedimento a seguir para excluí-lo. Certifique-se de alterar as VPCs que usam essas opções para outro conjunto de opções ou nenhuma opção. Para obter mais informações, consulte the section called “Alterar o conjunto de opções DHCP utilizado por uma VPC” (p. 260) e the section called “Alterar uma VPC para não usar opções DHCP” (p. 261).

Para excluir um conjunto de opções DHCP

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha DHCP Options Sets.
3. Selecione o conjunto de opções DHCP a ser excluído e escolha Actions, Delete DHCP options set (Ações, excluir conjunto de opções DHCP).

4. Na caixa de diálogo de confirmação, digite delete (excluir) e escolha Delete DHCP options set (Excluir conjunto de opções DHCP).

Visão geral da API e dos comandos

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 uma lista das APIs disponíveis, consulte Acessar a Amazon VPC (p. 1).

Criar um conjunto de opções DHCP para a sua VPC

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

Associar um conjunto de opções DHCP com a VPC especificada ou nenhuma opção DHCP

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

Descrever um ou mais conjuntos de opções DHCP

- describe-dhcp-options (CLI da AWS)
- Get-EC2DhcpOption (AWS Tools for Windows PowerShell)

Excluir um conjunto de opções DHCP

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

Usar DNS com a 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 de DNS determinam os nomes de host DNS de acordo com os endereços IP correspondentes.

Os endereços IPv4 públicos habilitam a comunicação pela Internet, enquanto os endereços IPv4 privados habilitam a comunicação na rede da instância (EC2-Classic ou VPC). Para obter mais informações, consulte Endereçamento IP na sua VPC (p. 117).

Fornecemos um servidor DNS (o Amazon Route 53 Resolver (p. 258)) à VPC. Para usar um servidor de DNS próprio, crie um novo conjunto de opções de DHCP para sua VPC. Para obter mais informações, consulte Conjuntos de opções de DHCP (p. 257).

Tópicos

- Nomes de hosts DNS (p. 263)
- Suporte a DNS em sua VPC (p. 263)
- Cotas de DNS (p. 264)
- Visualizar nomes de host DNS para a instância do EC2 (p. 265)

- Visualizar e atualizar o suporte a DNS para a VPC (p. 266)
- Usar zonas hospedadas privadas (p. 266)

Nomes de hosts DNS

Fornecemos à instância em uma VPC nomes de host DNS públicos e privados que correspondem aos endereços IPv4 públicos e IPv4 privados da instância. Não fornecemos nomes de host DNS para endereços IPv6.

Nomes de host DNS privados

Um nome de host DNS privado (interno) é resolvido para o endereço IPv4 privado da instância. O nome de host DNS privado assume o formulário `ip-`*`private-ipv4-address`*`.ec2.internal` para a região `us-east-1` e `ip-`*`private-ipv4-address`*`.`*`region`*`.compute.internal` para outras regiões (onde *`private-ipv4-address`* é o endereço IP de pesquisa inversa). Você pode usar o nome de host DNS privado para comunicação entre instâncias na mesma rede, mas não podemos determinar o nome de host DNS fora da rede em que a instância se encontra.

Quando você executa uma instância em uma VPC, ela sempre recebe um nome de host DNS privado.

Nomes de host DNS públicos

Um nome de host DNS público (externo) assume a forma `ec2-`*`public-ipv4-address`*`.compute-1.amazonaws.com` para a região `us-east-1` e `ec2-`*`public-ipv4-address`*`.`*`region`*`.compute.amazonaws.com` para outras regiões. O servidor DNS da Amazon resolve o nome de host DNS público para o endereço IPv4 público da instância fora da rede da instância e para o endereço IPv4 privado da instância dentro da rede da instância. Para obter mais informações, consulte Endereços IPv4 públicos e nomes de host DNS externos no Guia do usuário do Amazon EC2 para instâncias do Linux.

Quando você executa uma instância em uma VPC, ela receberá um nome de host DNS público se tiver um endereço IPv4 público e se os nomes de host DNS e os atributos de suporte de DNS para a VPC estiverem definidos como `true`. Para obter mais informações, consulte Suporte a DNS em sua VPC (p. 263).

Suporte a DNS em sua VPC

A VPC tem atributos que determinam se instâncias executadas na VPC recebem nomes de host DNS públicos que correspondem aos seus endereços IP públicos, e se a resolução de DNS pelo servidor DNS da Amazon é compatível com a VPC.

Atributo	Descrição
`enableDnsHostnames`	Indica se as instâncias com endereços IP públicos obtêm nomes de host DNS públicos correspondentes. Se esse atributo for `true`, as instâncias na VPC receberão nomes de host DNS públicos, mas somente se o atributo `enableDnsSupport` também for definido como `true`.
`enableDnsSupport`	Indica se há suporte para a resolução de DNS. Se o atributo for `false`, o servidor do Amazon Route 53 Resolver que determina nomes de

Atributo	Descrição
	host DNS públicos para endereços IP não estará habilitado. Se o atributo for `true`, haverá consultas ao servidor de DNS fornecido pela Amazon no endereço IP 169.254.169.253 ou no endereço IP reservado na base do intervalo de rede IPv4 da VPC "mais dois". Para obter mais informações, consulte Servidor DNS da Amazon (p. 258).

As seguintes regras se aplicam:

- Se ambos os atributos estiverem definidos como `true`, ocorrerá o seguinte:
  - Instâncias com um endereço IP público recebem nomes de host DNS públicos correspondentes.
  - O servidor do Amazon Route 53 Resolver pode determinar nomes de host DNS privados.
- Se um ou ambos os atributos estiverem definidos como `false`, ocorrerá o seguinte:
  - Instâncias com um endereço IP público não receberão nomes de host DNS públicos correspondentes.
  - O Amazon Route 53 Resolver não pode determinar nomes de host DNS privados.
  - As instâncias receberão nomes de host DNS privados personalizados se houver um nome de domínio personalizado no conjunto de opções DHCP (p. 257). Se não estiver usando o servidor do Amazon Route 53 Resolver, os 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 VPC endpoints 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 da 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 AWS Support.

Por padrão, ambos os atributos são definidos como `true` em uma VPC padrão ou em uma VPC criada pelo assistente. Por padrão, somente o atributo `enableDnsSupport` está definido como `true` em uma VPC criada de qualquer outra maneira. Para verificar se a VPC está habilitada para esses atributos, consulte Visualizar e atualizar o suporte a DNS para a VPC (p. 266). Se ativar o suporte a nomes de host DNS e DNS em uma VPC que anteriormente não recebia suporte, uma instância que você já tiver executado nessa VPC obterá um nome de host DNS público se tiver um endereço IPv4 público ou um endereço IP elástico.

Cotas de DNS

Cada instância do EC2 limita o número de pacotes que podem ser enviados para o Amazon Route 53 Resolver (especificamente endereços .2, como 10.0.0.2 e 169.254.169.253), até no máximo 1024 pacotes por segundo por interface de rede. Essa cota não pode ser aumentada. O número de consultas DNS por segundo ao qual o resolvedor do Amazon Route 53 oferece suporte 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 dimensionável, consulte o whitepaper Hybrid Cloud DNS Solutions for Amazon VPC.

Se você atingir a cota, o Amazon Route 53 Resolver rejeitará o tráfego. Algumas dos motivos para atingir a cota podem ser um problema de limitação de DNS ou consultas de metadados de instância que usam a interface de rede do Amazon 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 DNS fornecido pela Amazon falham devido à limitação de DNS da VPC?. Para obter instruções sobre a recuperação de metadados de instância, consulte Recuperar metadados de instância no Guia do usuário do Amazon EC2 para instâncias Linux.

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.

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 obter mais informações, consulte the section called “Suporte a DNS em sua VPC” (p. 263).

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

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar a Amazon VPC (p. 1).

- describe-instances (CLI da AWS)
- 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

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar a Amazon VPC (p. 1).

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

Visualizar e atualizar o suporte a DNS para a VPC

É possível visualizar e atualizar os atributos de suporte a DNS para a VPC usando o console da Amazon 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, selecione Your VPCs (Suas VPCs).
3. Selecione uma VPC na lista.
4. Revise as informações na guia Description (Descrição). Nesse exemplo, ambas as configurações estão habilitadas.

DNS resolution	Enabled
DNS hostnames	Enabled

5. Para atualizar essas configurações, escolha Actions e Edit DNS Resolution ou Edit DNS Hostnames. Na caixa de diálogo que se abre, selecione ou desmarque a caixa de seleção para ativar ou desativar o recurso. Em seguida, escolha Save changes (Salvar alterações).

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

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar a Amazon VPC (p. 1).

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

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

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar a Amazon VPC (p. 1).

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

Usar zonas hospedadas privadas

Se desejar acessar recursos na VPC usando nomes de domínio de DNS personalizados, como exemplo.com, em vez de endereços IPv4 privados ou nomes de host DNS privados fornecidos pela AWS, será possível 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.)

Você pode acessar uma zona hospedada privada de uma instância do EC2-Classic que esteja vinculada à sua VPC usando o ClassicLink, desde que sua VPC tenha permissão para receber suporte do DNS ClassicLink. Para obter mais informações, consulte Habilitar suporte a DNS ClassicLink no Guia do usuário do Amazon EC2 para instâncias do Linux. Do contrário, as 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. Para obter mais informações, consulte Limitações do ClassicLink no Guia do usuário do Amazon EC2 para instâncias do Linux.

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

Listas de prefixos

Uma lista de prefixos é um conjunto de um ou mais blocos CIDR. Existem dois tipos de listas de prefixos:

- Lista de prefixos gerenciados pela AWS: representa os intervalos de endereços IP de um serviço da AWS. Você pode fazer referência a uma lista de prefixos gerenciados pela AWS nas regras do grupo de segurança da VPC e nas entradas da tabela de rotas da sub-rede. Por exemplo, você pode fazer referência a uma lista de prefixos gerenciados pela AWS em uma regra de saída do grupo de segurança da VPC ao se conectar a um serviço da AWS por meio de um VPC endpoint do gateway. Não é possível criar, modificar, compartilhar ou excluir uma lista de prefixos gerenciados pela AWS.
- Lista de prefixos gerenciados pelo cliente: um conjunto de blocos CIDR IPv4 ou IPv6 definidos e gerenciados por você. É possível fazer referência à lista de prefixos nas regras do grupo de segurança da VPC, nas entradas da tabela de rotas da sub-rede e nas entradas da tabela de rotas do gateway de trânsito. Isso permite o gerenciamento dos endereços IP usados com frequência para esses recursos em um único grupo, em vez de fazer referência repetidamente aos mesmos endereços IP em cada recurso. 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.

Os tópicos a seguir descrevem como criar e trabalhar com listas de prefixos gerenciados pelo cliente.

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.

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

- Ao criar uma lista de prefixos, você deve especificar o número máximo de entradas com as quais a lista de prefixos é compatível. Não é possível modificar o número máximo de entradas posteriormente.
- Quando você faz referência a uma lista de prefixos em um recurso, o número máximo de entradas para as listas de prefixos é considerado equivalente ao número de entradas para o recurso. Por exemplo, se você cria uma lista de prefixos com até 20 entradas e faz referência a essa lista de prefixos em uma regra de grupo de segurança, isso conta como 20 regras para o grupo de segurança.

- Você pode modificar uma lista de prefixos adicionando ou removendo entradas ou alterando seu nome.
- 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.
- Há cotas relacionadas a listas de prefixos. Para obter mais informações, consulte Cotas da Amazon VPC (p. 345).
- Quando você faz referência a uma lista de prefixos em uma tabela de rotas, as regras de prioridade da rota se aplicam. Para obter mais informações, consulte Prioridade de rotas para listas de prefixos (p. 291).
- Uma lista de prefixos só se aplica à Região em que você a criou. Por exemplo, se você criar uma lista em `us-east-1`, ela não estará disponível em `eu-west-1`.
- Não é possível fazer referência à lista de prefixos nas regras do grupo de segurança do EC2 Classic.

As regras a seguir se aplicam às listas de prefixos gerenciados pela AWS:

- Não é possível criar, modificar, compartilhar ou excluir uma lista de prefixos gerenciados pela AWS.
- Quando você faz referência a uma lista de prefixos gerenciados pela AWS em um recurso, ela conta como uma única regra ou entrada para o recurso.
- Não é possível visualizar o número da versão de uma lista de prefixos gerenciados pela AWS.

Antes de trabalhar com listas de prefixos, revise as cotas das the section called “Listas de prefixos gerenciadas pelo cliente” (p. 346).

Versões da lista de prefixos

Uma lista de prefixos pode ter várias versões. Toda vez que você adiciona ou remove entradas de uma lista de prefixos, nós 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 para uma nova versão.

Trabalhar com listas de prefixos

Os tópicos a seguir descrevem como criar e trabalhar com listas de prefixos gerenciados pelo cliente. É possível trabalhar com listas de prefixos usando o console da Amazon VPC ou a CLI da AWS.

Tópicos

Criar uma lista de prefixos

Ao criar uma nova lista de prefixos, você deve especificar o número máximo de entradas com as quais a lista de prefixos é compatível. Certifique-se de especificar um número máximo de entradas que atenda às suas necessidades, pois não será possível alterar esse número posteriormente.

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 CLI da AWS

Use o comando create-managed-prefix-list.

Visualizar listas de prefixos

É possível visualizar listas de prefixos, listas de prefixos compartilhadas com você e listas de prefixos gerenciadas pela AWS usando o console da Amazon VPC ou a CLI da 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 Owner ID (ID do proprietário) mostra o ID de conta da AWS do proprietário da lista de prefixos. Para listas de prefixos gerenciados pela AWS, o ID do proprietário é AWS.

Como visualizar listas de prefixos com a CLI da AWS

Use o comando describe-managed-prefix-lists.

Visualizar as entradas de uma lista de prefixos

É possível visualizar as entradas de uma lista de prefixos usando o console da Amazon VPC ou a CLI da 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. Selecione a 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 CLI da AWS

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.

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. Selecione a 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 CLI da AWS

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

Modificar uma lista de prefixos (adicionando e removendo entradas)

É possível modificar o nome da sua lista de prefixos e adicionar ou remover entradas.

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

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. Selecione a lista de prefixos e escolha Ações, 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 CLI da AWS

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 de lista de prefixos para uma nova versão.

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. Selecione a lista de prefixos e escolha Ações, Restaurar lista de prefixos.
4. Na lista suspensa, escolha a versão da lista de prefixos.
5. Escolha Restaurar lista de prefixos.

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

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. Para visualizar as referências à sua lista de prefixos, consulte Visualizar associações (referências) para a lista de prefixos (p. 269).

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 CLI da AWS

Use o comando delete-managed-prefix-list.

Referenciar listas de prefixos nos recursos da AWS

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

Subnet route tables

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 Tabelas de rotas para sua VPC (p. 283).

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). Em Destino, insira o ID de uma lista de prefixos.
5. Em Target (alvo), escolha um alvo.
6. Escolha Save routes (Salvar rotas).

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

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

VPC security groups

É possível especificar uma lista de prefixos como origem de uma regra de entrada ou como destino de uma regra de saída. Para mais informações sobre security groups, consulte Grupos de segurança para a VPC (p. 180).

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 o ID da lista de prefixos.
6. Selecione Save rules (Salvar regras).

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

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`.

Transit gateway route tables

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.

Identity and Access Management para as listas de prefixos

Por padrão, os usuários do IAM não têm permissão para criar, visualizar, modificar nem excluir listas de prefixos. É possível criar uma política do IAM que permita que os usuários trabalhem com listas de prefixos.

Para ver uma lista de ações da Amazon VPC e os recursos e chaves de condição que podem ser usados em uma política do IAM, consulte Ações, recursos e chaves de condição do Amazon EC2 no Guia do usuário do IAM.

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:DescribeManagedPrefixLists",
        "ec2:ModifyManagedPrefixList",
        "ec2:GetManagedPrefixListEntries",
        "ec2:RestoreManagedPrefixListVersion",
        "ec2:GetManagedPrefixListAssociations"
      ],
      "Resource": "arn:aws:ec2:region:account:prefix-list/pl-123456abcde123456"
    }
   ]
}
```

Para obter mais informações sobre como trabalhar com o IAM na Amazon VPC, consulte Identity and Access Management para o Amazon VPC (p. 162).

Trabalhar com listas de prefixos compartilhadas

As listas de prefixos gerenciadas pelo cliente se integram ao AWS Resource Access Manager (AWS RAM). Com o AWS RAM, você compartilha recursos que possui nas contas da AWS criando um

compartilhamento de recursos. Ele especifica os recursos a serem compartilhados e os consumidores com os quais compartilhá-los. Os consumidores podem ser contas individuais da AWS, unidades organizacionais ou toda uma organização do AWS Organizations.

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

O proprietário de uma lista de prefixos pode compartilhar uma lista de prefixos com:

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

Tópicos

Pré-requisitos para compartilhamento de listas de prefixos

- Para compartilhar uma lista de prefixos, é necessário ser o proprietário dela em sua conta da AWS. 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 sua organização ou uma unidade organizacional no AWS Organizations, é necessário habilitar o compartilhamento com o AWS Organizations. Para obter mais informações, consulte Habilitar compartilhamento com o AWS Organizations no Guia do usuário do AWS RAM.

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.

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

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 Guia 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 de sua propriedade a um compartilhamento de recursos existente, siga as etapas em Atualizar um compartilhamento de recursos no Guia 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 CLI da AWS

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

- create-resource-share
- associate-resource-share
- update-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 CLI da AWS.

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 Owner ID (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 CLI da AWS

Use o comando describe-managed-prefix-lists. O comando retorna as listas de prefixos de sua propriedade e as listas de prefixos compartilhadas com você. `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 e que fazem referência a uma lista de prefixos compartilhada usando o console da Amazon VPC e a CLI da AWS.

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 CLI da AWS

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

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 (p. 274). 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 de sua propriedade, é necessário removê-la do compartilhamento de recursos. É possível fazer isso usando o console da AWS RAM ou a CLI da AWS.

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

Consulte Atualizar um compartilhamento de recursos no Guia do usuário do AWS RAM.

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

Use o comando disassociate-resource-share.

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.

Faturamento e medição

Não há cobranças adicionais pelo compartilhamento de listas de prefixos.

Cotas

Para obter mais informações sobre cotas (limites) relacionadas ao AWS RAM, consulte Limites de serviço no Guia do usuário do AWS RAM.

Componentes de rede do Amazon EC2

Você pode usar os seguintes componentes de rede do Amazon EC2 para configurar redes em sua VPC.

Componentes

Interfaces de rede elástica

Uma interface de rede elástica (chamada interface de rede nesta documentação) é um componente lógico de redes em uma VPC que representa um cartão de rede virtual. Ele pode incluir os seguintes atributos:

- Endereço IPv4 privado primário
- Endereços IPv4 privados secundários
- Um endereço IP elástico por endereço IPv4 privado
- Um endereço IPv4 público, que pode ser autoatribuído à interface de rede para eth0 quando você executa uma instância
- Um ou mais endereços IPv6
- Um ou mais security groups
- Endereço MAC
- Indicador de verificação de origem/destino
- Descrição

Você pode criar uma interface de rede, anexá-la a uma instância, separá-la de uma instância e anexá-la a outra instância. Os atributos de uma interface seguem o processo, pois estão anexados ou separados de uma instância e reanexados a uma outra instância. Quando você migra uma interface de rede de uma instância para outra, o tráfego da rede é redirecionado para a nova instância.

Cada instância na VPC possui uma interface de rede padrão (a interface de rede primária) à qual está atribuído um endereço IPv4 privado do intervalo de endereços IPv4 da VPC. Não é possível separar uma interface de rede primária de uma instância. Você pode criar e anexar uma interface de rede adicional para qualquer instância da VPC. O número de interfaces de rede que você pode anexar varia de acordo com o tipo de instância. Para obter mais informações, consulte Endereços IP por interface de rede por tipo de instância no Guia do usuário do Amazon EC2 para instâncias do Linux.

Associar várias interfaces de rede a uma instância é útil quando você deseja:

- Criar uma rede de gerenciamento.
- Usar dispositivos de rede e segurança na VPC.
- Criar instâncias dual-homed com cargas de trabalho/funções em sub-redes distintas.

- Criar uma solução de baixo orçamento e alta disponibilidade.

Para obter mais informações sobre as interfaces de rede e as instruções para trabalhar com elas usando o console do Amazon EC2, consulte Interfaces de rede elástica no Guia do usuário do Amazon EC2 para instâncias do Linux.

Endereços IP elásticos

Um endereço IP elástico é um endereço IPv4 público estático projetado para computação em nuvem dinâmica. É possível associar um endereço IP elástico a qualquer instância ou interface de rede em qualquer VPC em sua conta. Com um endereço IP elástico, você pode mascarar a falha de uma instância remapeando rapidamente o endereço para outra instância na VPC.

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 para instâncias do Linux.

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 eth0 de sua instância, o endereço IPv4 público atual (se houver um) será liberado ao grupo de endereços IP públicos da EC2-VPC. Se você associar um endereço IP elástico, em poucos minutos a interface de rede eth0 será automaticamente atribuída a um endereço IPv4 público. Isso não se aplica se você tiver anexado uma segunda interface de rede à sua instância.
- Para garantir o uso eficiente dos endereços IP elásticos, aplicamos uma pequena cobrança por hora quando eles não estão associados a uma instância em execução ou quando eles estão associados a uma instância encerrada ou a uma interface de rede desvinculada. Enquanto a instância estiver em execução, você não será cobrado por um endereço IP elástico associado a essa instância, mas será cobrado por outros endereços IP elásticos associados a ela. Para obter mais informações, consulte Definição de preço do Amazon EC2.
- 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 Dispositivos NAT para sua VPC (p. 228).
- 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 obter mais informações, consulte the section called “Grupos de segurança” (p. 180) e the section called “Network ACLs” (p. 190).
- 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. Este é o local do qual anunciamos o bloco CIDR. Definir o grupo de borda de rede limita o bloco CIDR a este 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 para instâncias do Linux.

Existem diferenças entre um endereço IP elástico usado em uma VPC e um usado no EC2-Classic. Para obter mais informações, consulte Diferenças entre o EC2-Classic e a VPC no Guia do usuário do Amazon EC2 para instâncias do Linux. É possível mover um endereço IP elástico alocado para uso na plataforma EC2-Classic para a plataforma da VPC. Para obter mais informações, consulte Migrar um endereço IP elástico do EC2-Classic.

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.

Trabalhar com endereços IP elásticos

As seções a seguir descrevem como você pode trabalhar com endereços IP elásticos.

Tarefas

Como alocar um endereço IP elástico

Antes de usar um IP elástico, é necessário alocar um para uso em sua VPC.

Console

Para alocar um endereço IP elástico para uso em uma VPC

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 Allocate Elastic IP address (Alocar endereço IP elástico).
4. 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 conjunto de endereços IPv4 públicos): se você deseja alocar um endereço IPv4 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.

5. (Opcional) Adicione ou remova uma tag.

   [Adicionar uma tag] Escolha Adicionar nova tag e faça o seguinte:

   - Em Key (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.
6. Escolha Allocate.

   Note

   Se sua conta for compatível com o EC2-Classic, escolha primeiro VPC.

CLI and API

Para alocar um endereço IP elástico

- allocate-address (CLI da AWS)
- New-EC2Address (AWS Tools for Windows PowerShell)

Como 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 Usar DNS com a VPC (p. 262).

Console

Como associar um endereço IP elástico a uma instância ou interface de rede em uma VPC

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

CLI and API

Como associar um endereço IP elástico a uma instância ou interface de rede

- associate-address (CLI da AWS)
- Register-EC2Address (AWS Tools for Windows PowerShell)

Visualizar endereços IP elásticos

É possível visualizar os endereços IP elásticos alocados à sua conta.

Console

Como visualizar endereços IP elásticos

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Elastic IPs (IPs elásticos).
3. Para filtrar a lista exibida, comece a digitar parte do endereço IP elástico ou um de seus atributos na caixa de pesquisa.

CLI and API

Como visualizar um ou mais endereços IP elásticos

- describe-addresses (CLI da AWS)
- Get-EC2Address (AWS Tools for Windows PowerShell)

Atribuir tags a um endereço IP elástico

Você pode aplicar tags ao seu endereço IP elástico para ajudar a identificá-lo ou categorizá-lo de acordo com as necessidades da sua organização.

Console

Para aplicar uma tag em 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 selecione Tags.
4. Escolha Manage tags (Gerenciar tags), insira as chaves e os valores de tag conforme necessário e escolha Save (Salvar).

CLI and API

Para aplicar uma tag em um endereço IP elástico

- create-tags (CLI da AWS)
- New-EC2Tag (AWS Tools for Windows PowerShell)

Desassociar 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.

Console

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, selecione 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).

CLI and API

Para dissociar um endereço IP elástico

- disassociate-address (CLI da AWS)
- Unregister-EC2Address (AWS Tools for Windows PowerShell)

Liberar um endereço IP elástico

Se não for mais necessário um endereço IP elástico, recomendamos liberá-lo. Você será cobrado pelo endereço IP elástico que estiver alocado para uso com uma VPC e não estiver associado a uma instância. O endereço IP elástico não deve ser associado a uma instância ou interface de rede.

Console

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, selecione 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.

CLI and API

Para liberar um endereço IP elástico

- release-address (CLI da AWS)
- Remove-EC2Address (AWS Tools for Windows PowerShell)

Recuperar um endereço IP elástico

Se liberar o endereço IP elástico, você poderá 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 cota.

É possível recuperar um endereço IP elástico usando a API do Amazon EC2 ou uma ferramenta de linha de comando.

Como recuperar um endereço IP elástico usando a CLI da AWS

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
```

ClassicLink

O ClassicLink permite unir uma instância do EC2-Classic a uma VPC na sua conta, dentro da mesma região. Isso permite a associação dos grupos de segurança da VPC à instância do EC2-Classic, permitindo a comunicação entre a instância do EC2-Classic e as instâncias na VPC, usando endereços IPv4 privados. Com o ClassicLink, não há necessidade de usar endereços IPv4 públicos ou endereços IP elásticos para

permitir a comunicação entre instâncias nestas plataformas. Para obter mais informações sobre endereços IPv4 público e privado, consulte Endereçamento IP na sua VPC (p. 117).

O ClassicLink está disponível para todos os usuários com contas que oferecem suporte à plataforma do EC2-Classic e pode ser usado com qualquer instância do EC2-Classic.

Não há cobrança adicional pelo uso do ClassicLink. Aplicam-se as cobranças padrão pela transferência de dados e pela utilização de horas de instância.

Para obter mais informações sobre o ClassicLink e como usá-lo, consulte os seguintes tópicos no Guia do usuário do Amazon EC2:

- Noções básicas do ClassicLink
- Limitações do ClassicLink
- Trabalhar com o ClassicLink
- Visão geral da CLI e da API do ClassicLink

Tabelas de rotas para sua VPC

Uma tabela de rotas contém um conjunto de regras, denominado rotas, que são usadas para determinar para onde o tráfego de rede de sua sub-rede ou gateway é direcionado.

Tópicos

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.
- 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.
- 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.
- Tabela de rotas de gateway: uma tabela de rotas associada a um gateway da Internet ou gateway privado virtual.
- Tabela de rotas de gateway local: uma tabela de rotas associada a um gateway local do Outposts. Para obter informações sobre gateways locais, consulte Gateways locais no Guia do usuário do AWS Outposts.
- 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`.
- Propagation (Propagação): a propagação das rotas permite que um gateway privado virtual propague automaticamente rotas para as tabelas de rotas. Isso significa que você não precisa inserir manualmente rotas VPN para suas tabelas de rotas. Para mais informações sobre as opções de roteamento VPN, consulte Opções de roteamento do Site-to-Site VPN no Guia do usuário do Site-to-Site VPN.
- 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.
- Local route (Rota local): uma rota padrão para comunicação dentro da VPC.

Para obter exemplos de opções de roteamento, consulte the section called “Exemplo de opções de roteamento” (p. 291).

Como funcionam as tabelas de rotas

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.

Você tem a opção de associar uma tabela de rotas a um gateway da Internet ou a um gateway privado virtual (tabela de rotas de gateway). Isso permite que você especifique regras de roteamento para o tráfego de entrada que entra na VPC por meio do gateway. Para obter mais informações, consulte Tabelas de rotas do gateway (p. 288).

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 obter mais informações, consulte Cotas da Amazon VPC (p. 345).

Tópicos

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.

Destino	Destino
0.0.0.0/0	igw-12345678901234567

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.

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.

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. Você não pode modificar ou excluir essas rotas em uma tabela de rotas de sub-rede ou na tabela de rotas principal.

Para obter mais informações sobre rotas e rotas locais em uma tabela de rotas de gateway, consulte Tabelas de rotas do gateway (p. 288).

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.

No exemplo a seguir, um bloco CIDR IPv6 é associado à VPC. Na tabela de rotas:

- O tráfego IPv6 destinado a permanecer dentro da VPC (`2001:db8:1234:1a00::/56`) é coberto pela rota `Local` e é roteado dentro da VPC.
- Os tráfegos IPv4 e IPv6 são tratados separadamente; por isso, todo tráfego IPv6 (exceto pelo tráfego dentro da VPC) é roteado para o gateway da Internet apenas de saída.
- Há uma rota para tráfego IPv4 `172.31.0.0/16` que direciona para uma conexão emparelhada.
- Existe uma rota para todo o tráfego IPv4 (`0.0.0.0/0`) que direciona para um gateway da Internet.
- Há uma rota para todo o tráfego IPv6 (`::/0`) que direciona para um gateway da Internet apenas de saída.

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

Se fizer referência frequentemente ao mesmo conjunto de blocos CIDR nos recursos da AWS, você poderá criar uma lista de prefixos gerenciados pelo cliente (p. 267) para agrupá-los. Depois, você pode especificar a lista de prefixos como destino na entrada da tabela de rotas.

Tabela de rotas principal

Quando você cria uma VPC, a tabela de rotas principal é criada automaticamente. A tabela de rotas principal controla o roteamento para todas as sub-redes que não estejam explicitamente associadas com outra tabela de rotas. 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. Quando você usa o assistente de VPC no console para criar uma VPC não padrão com um gateway NAT ou gateway privado virtual, o assistente adiciona automaticamente rotas à tabela de rotas principal para esses gateways.

As seguintes regras se aplicam à 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 por uma tabela de rotas de sub-rede personalizada.
- Você pode adicionar, remover e modificar rotas na tabela de rotas principal.
- Não é possível criar uma rota que seja mais específica do que a rota local.
- 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 (p. 306).

Tabelas de rotas personalizadas

Por padrão, uma tabela de rotas personalizada fica vazia e você adiciona rotas conforme necessário. Quando você usa o assistente de VPC no console para criar uma VPC com um gateway da Internet, o assistente cria uma tabela de rotas personalizada e adiciona uma rota ao 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 a uma tabela (p. 302).

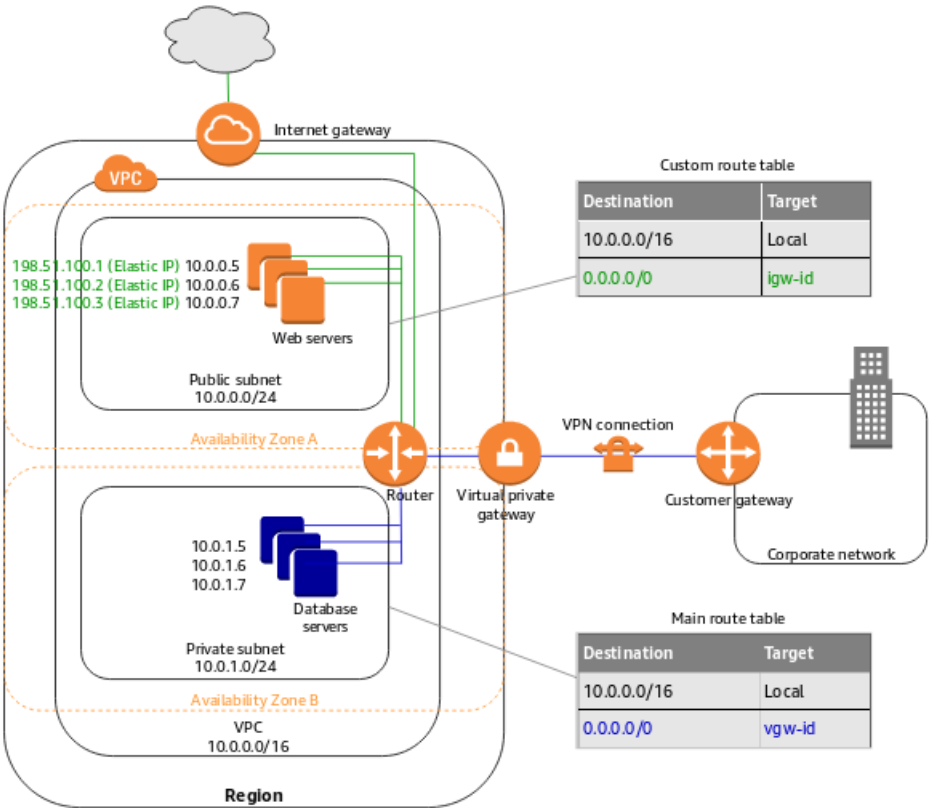
As sub-redes que estão em VPCs associadas ao Outposts podem ter um tipo de alvo adicional de um gateway local. Essa é a única diferença de roteamento das sub-redes que não são de Outposts.

Não é possível associar uma sub-rede a uma tabela de rotas se qualquer uma das seguintes situações se aplicar:

- A tabela de rotas contém uma rota existente que é mais específica do que a rota local padrão.
- O alvo da rota local padrão foi substituído.

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 principal tem uma rota para o gateway privado virtual. Uma tabela de rotas personalizada é explicitamente associada à sub-rede pública. A tabela de rotas personalizada tem uma rota para a Internet (`0.0.0.0/0`) por meio do gateway da Internet.

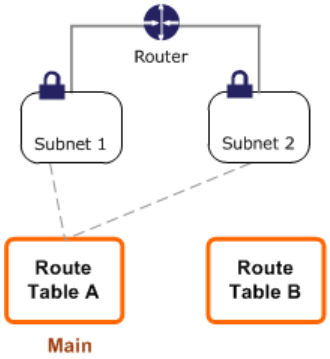


Se criar uma nova sub-rede nessa VPC, ela será automaticamente e implicitamente associada à tabela de rotas principal, que roteia o tráfego para o gateway privado virtual. Se definir uma configuração inversa (em que a tabela de rotas principal tem a rota para o gateway da Internet e a tabela de rotas personalizada tem a rota para o gateway privado virtual), uma nova sub-rede automaticamente terá uma rota para o gateway da Internet.

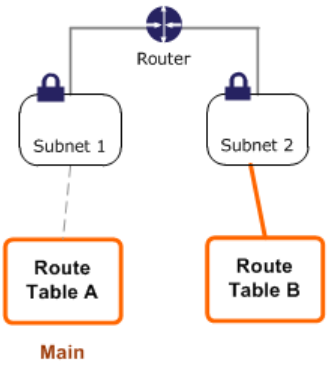
Exemplo 2: Substituir a tabela de rotas principal

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.

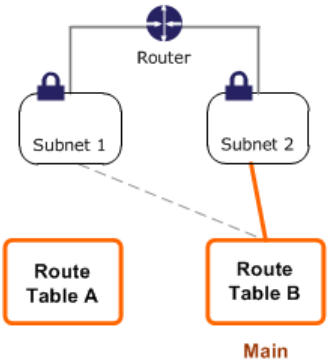
O diagrama a seguir mostra uma VPC com duas sub-redes que estão implicitamente associadas à tabela de rotas principal (Tabela de rotas A) e uma tabela de rotas personalizada (Tabela de rotas B), que não está associada a nenhuma sub-rede.



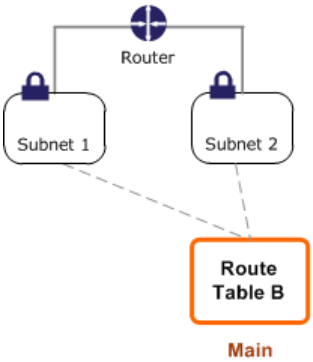
Você pode criar uma associação explícita entre a Sub-rede 2 e a Tabela de rotas B.



Depois que testar a Tabela de rotas B, poderá torná-la a tabela de rotas principal. Observe que a Sub-rede 2 ainda tem uma associação explícita com a Tabela de rotas B e a Sub-rede 1 tem uma associação implícita com a Tabela de rotas B porque é a nova tabela de rotas principal. A Tabela de rotas A não está mais sendo usada.



Se dissociar a Sub-rede 2 da Tabela de rotas B, ainda assim haverá uma associação implícita entre a Sub-rede 2 e a Tabela de rotas B. Se 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.

Uma tabela de rotas de gateway oferece suporte a rotas em que o destino seja `local` (a rota local padrão), um endpoint do Gateway Load Balancer ou uma interface de rede elástica (interface de rede) na VPC associada ao 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 obter mais informações, consulte Substituir e restaurar o alvo de uma rota local (p. 307).

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

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.
- Não é possível rotear o tráfego de um gateway privado virtual para um endpoint do Gateway Load Balancer . Se você associar sua tabela de rotas a um gateway privado virtual e adicionar uma rota com um endpoint do Gateway Load Balancer como destino, o tráfego destinado ao endpoint será descartado.
- 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 um 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 (p. 297).
- 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.

Para obter um exemplo de roteamento para um dispositivo de segurança, consulte Roteamento para um dispositivo Middlebox em sua VPC (p. 297).

Prioridade de rota

Para determinar como o tráfego deve ser roteado, usamos a rota mais específica em sua tabela de rotas que corresponde ao tráfego (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.

Por exemplo, a 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

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 as rotas propagadas se sobrepuserem às rotas estáticas e a correspondência de prefixo mais longa não puder ser aplicada, as rotas estáticas terão prioridade sobre as rotas propagadas. Para mais informações, consulte Tabelas de rotas e prioridade de rotas VPN no Guia do usuário do AWS Site-to-Site VPN.

Nesse exemplo, a tabela de rotas tem uma rota estática para um gateway da Internet (que foi adicionado manualmente) e uma rota propagada para um gateway privado virtual. O destino de ambas as rotas é `172.31.0.0/24`. Nesse caso, todo tráfego destinado para `172.31.0.0/24` é roteado para o gateway da Internet – é uma rota estática e, portanto, tem prioridade sobre a rota propagada.

Destino	Destino
10.0.0.0/16	Local
172.31.0.0/24	vgw-11223344556677889 (propagado)

Destino	Destino
172.31.0.0/24	igw-12345678901234567 (estático)

A mesma regra se aplica se a tabela de rotas contiver uma rota estática para qualquer uma das seguintes opções:

- gateway NAT
- Interface de rede
- ID da instância
- VPC endpoint de gateway
- Transit gateway
- Conexão de emparelhamento de VPC
- Endpoint do Gateway Load Balancer

Se os destinos das rotas estáticas e propagadas forem os mesmos, a rota estática terá prioridade.

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 que se sobreponha a outra rota que faça referência a uma lista de prefixos, a rota estática com o bloco CIDR de destino terá prioridade.
- Se a tabela de rotas contiver uma rota propagada que se sobreponha a uma rota que faz referência a uma lista de prefixos, a rota que faz referência à lista de prefixos terá prioridade.
- 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.
- Se o bloco CIDR em uma entrada de lista de prefixos não for válido para a tabela de rotas, a entrada será ignorada. Por exemplo, em uma tabela de rotas de sub-rede, se a lista de prefixos contiver uma entrada com um CIDR mais específico do que o CIDR da VPC, essa entrada será ignorada.

Exemplo de opções de roteamento

Os tópicos a seguir descrevem o roteamento para gateways específicos ou conexões em sua VPC.

Opções

- Roteamento com uma lista de prefixos (p. 299)
- Roteamento para um endpoint do Gateway Load Balancer (p. 299)

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 Gateways da Internet (p. 212).

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-xxxxxxxx; um intervalo de endereços IP específico para Amazon S3) é roteado para um VPC endpoint de gateway e o tráfego 10.25.0.0/16 é roteado para uma conexão de emparelhamento de VPC. Os intervalos de endereços IP pl-xxxxxxxx e 10.25.0.0/16 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 obter mais informações, consulte Gateways NAT (p. 229) e Instâncias NAT (p. 248). Não é possível usar dispositivos NAT para tráfego IPv6.

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 mais informações, consulte O que é o AWS Site-to-Site VPN? e Tabelas de rotas e prioridade de rotas da VPN no Guia 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 suporte para tráfego IPv6 roteado por meio de um gateway privado virtual para uma conexão do AWS Direct Connect. Para obter mais informações, consulte o Guia do usuário do AWS Direct Connect.

Roteamento para um gateway local do AWS Outposts

As sub-redes que estão em VPCs associadas ao AWS Outposts podem ter um tipo de alvo 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

Rotear para um gateway de operadora de zona do Wavelength

As sub-redes que estão em zonas do Wavelength podem ter um tipo de destino adicional de um gateway de operadora. Considere o caso em que você deseja que o gateway de operadora roteie o tráfego para rotear todo o tráfego que não seja da VPC para a rede da operadora. Para fazer isso, crie e anexe um gateway de operadora à sua VPC e adicione as seguintes rotas:

Destino	Destino
0.0.0.0/0	cagw-id
::/0	cagw-id

Roteamento para uma conexão de emparelhamento de VPC

Conexão de emparelhamento de 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 de 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 de 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 obter mais informações, consulte VPCs e sub-redes (p. 100). 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 de VPC para acessar todo ou parte do bloco CIDR IPv6 da VPC emparelhada.

Por exemplo, usando a mesma conexão de emparelhamento de 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 ClassicLink

O ClassicLink é um recurso que permite vincular uma instância do EC2-Classic a uma VPC, permitindo a comunicação entre a instância do EC2-Classic e instâncias na VPC usando endereços IPv4 privados. Para obter mais informações sobre o ClassicLink, consulte ClassicLink (p. 281).

Quando uma VPC é habilitada para o ClassicLink, é adicionada uma rota a todas as tabelas de rotas da sub-rede com os destinos `10.0.0.0/8` e `local`. Isso permite a comunicação entre instâncias da VPC e qualquer instância do EC2-Classic que estejam vinculadas à VPC. Se você adicionar outra tabela de rotas a uma VPC habilitada para o ClassicLink, ela receberá automaticamente uma rota com os destinos `10.0.0.0/8` e `local`. Se você desabilitar o ClassicLink para uma VPC, essa rota será excluída automaticamente de todas as tabelas de rotas da sub-rede.

Se qualquer uma das tabelas de rotas da sub-rede tiver rotas existentes para intervalos de endereços dentro do CIDR `10.0.0.0/8`, não será possível habilitar a VPC para o ClassicLink. Isso não inclui rotas locais para VPCs com intervalos de endereços IP `10.0.0.0/16` e `10.1.0.0/16`.

Se você já tiver habilitado uma VPC para o ClassicLink, pode ser que não consiga adicionar nenhuma rota mais específica às suas tabelas de rotas para o intervalo de endereços IP `10.0.0.0/8`.

Se modificar uma conexão de emparelhamento de VPC para permitir a comunicação entre instâncias em sua VPC e a Instância EC2-Classic que está vinculada à VPC emparelhada, uma rota estática será adicionada automaticamente às suas tabelas de rotas com os destinos `10.0.0.0/8` e `local`. Se modificar uma conexão de emparelhamento de VPC para permitir a comunicação entre uma Instância EC2-Classic local vinculada à sua VPC e a instâncias em uma VPC emparelhada, você deverá adicionar manualmente uma rota à sua tabela de rotas principal com um destino do bloco CIDR da VPC emparelhada e um destino da conexão de emparelhamento de VPC. A Instância EC2-Classic recorre à tabela de rotas principal para realizar o roteamento para a VPC emparelhada. Para obter mais informações, consulte Configurações com o ClassicLink no 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 Gateways da Internet apenas de saída (p. 218).

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 em sua VPC

Você pode 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 de middlebox na VPC. 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.

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 obter mais informações, consulte Tabelas de rotas do gateway (p. 288). Você também pode rotear o tráfego de saída da sub-rede para um dispositivo middlebox em outra sub-rede.

> Note
>
> Se você habilitou 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 haja 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 ofereça suporte a quadros jumbo).

Considerações sobre o dispositivo

É possível escolher um dispositivo de terceiros no 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 do destino no Guia do usuário do Amazon EC2 para instâncias do Linux.
- O encadeamento de serviço não é compatível.
- Você não pode rotear o tráfego entre hosts na mesma sub-rede por meio de um dispositivo.
- Você não pode rotear o tráfego entre sub-redes por meio de um dispositivo.
- O dispositivo não precisa executar a conversão de endereços de rede (NAT).
- Para interceptar tráfego IPv6, certifique-se de configurar sua VPC, sub-rede e o dispositivo para IPv6. Para obter mais informações, consulte Trabalhar com VPCs e sub-redes (p. 109). Gateways privados virtuais não oferecem suporte ao tráfego IPv6.

Configuração do roteamento do dispositivo

Para rotear o tráfego de entrada para um dispositivo, crie uma tabela de rotas e adicione uma rota que direcione o tráfego destinado a uma sub-rede à interface de rede do dispositivo. Esta rota é mais específica do que a rota local da tabela de rotas. Associe esta tabela de rotas ao seu gateway da Internet ou gateway privado virtual. A tabela de rotas a seguir roteia o tráfego IPv4 destinado a uma sub-rede para a interface de rede do dispositivo.

Destino	Destino
10.0.0.0/16	Local
10.0.1.0/24	eni-id

Como alternativa, você pode substituir o alvo 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 adicionadas à VPC posteriormente.

Destino	Destino
10.0.0.0/16	eni-id

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	Destino
10.0.0.0/16	Local
0.0.0.0/0	eni-id

Na tabela de rotas associada à sub-rede do dispositivo, adicione uma rota que roteie o tráfego de volta para o gateway da Internet ou para o gateway privado virtual.

Destino	Destino
10.0.0.0/16	Local
0.0.0.0/0	igw-id

Você pode aplicar a mesma configuração de roteamento para tráfego IPv6. Por exemplo, na tabela de rotas do gateway, você pode substituir o alvo das rotas locais IPv4 e IPv6 pela interface de rede do dispositivo.

Destino	Destino
10.0.0.0/16	eni-id
2001:db8:1234:1a00::/56	eni-id

No diagrama a seguir, um dispositivo de firewall é instalado e configurado em uma instância do Amazon EC2 na sub-rede A em sua VPC. O dispositivo inspeciona todo o tráfego que entra e sai da VPC pelo gateway da Internet. A tabela de rotas A está associada ao gateway da Internet. O tráfego destinado à sub-rede B que entra na VPC por meio do gateway da Internet é roteado para a interface de rede do dispositivo (`eni-11223344556677889`). Todo o tráfego que sai da sub-rede B também é roteado para a interface de rede do dispositivo.

O exemplo a seguir tem a mesma configuração do exemplo anterior, mas inclui tráfego IPv6. O tráfego IPv6 destinado à sub-rede B que entra na VPC pelo gateway da Internet é roteado para a interface de rede do dispositivo (`eni-11223344556677889`). Todo o tráfego (IPv4 e IPv6) que sai da sub-rede B também é roteado para a interface de rede do dispositivo.

Roteamento com uma lista de prefixos

Se fizer referência frequentemente ao mesmo conjunto de blocos CIDR nos recursos da AWS, você poderá criar uma lista de prefixos gerenciados pelo cliente (p. 267) 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

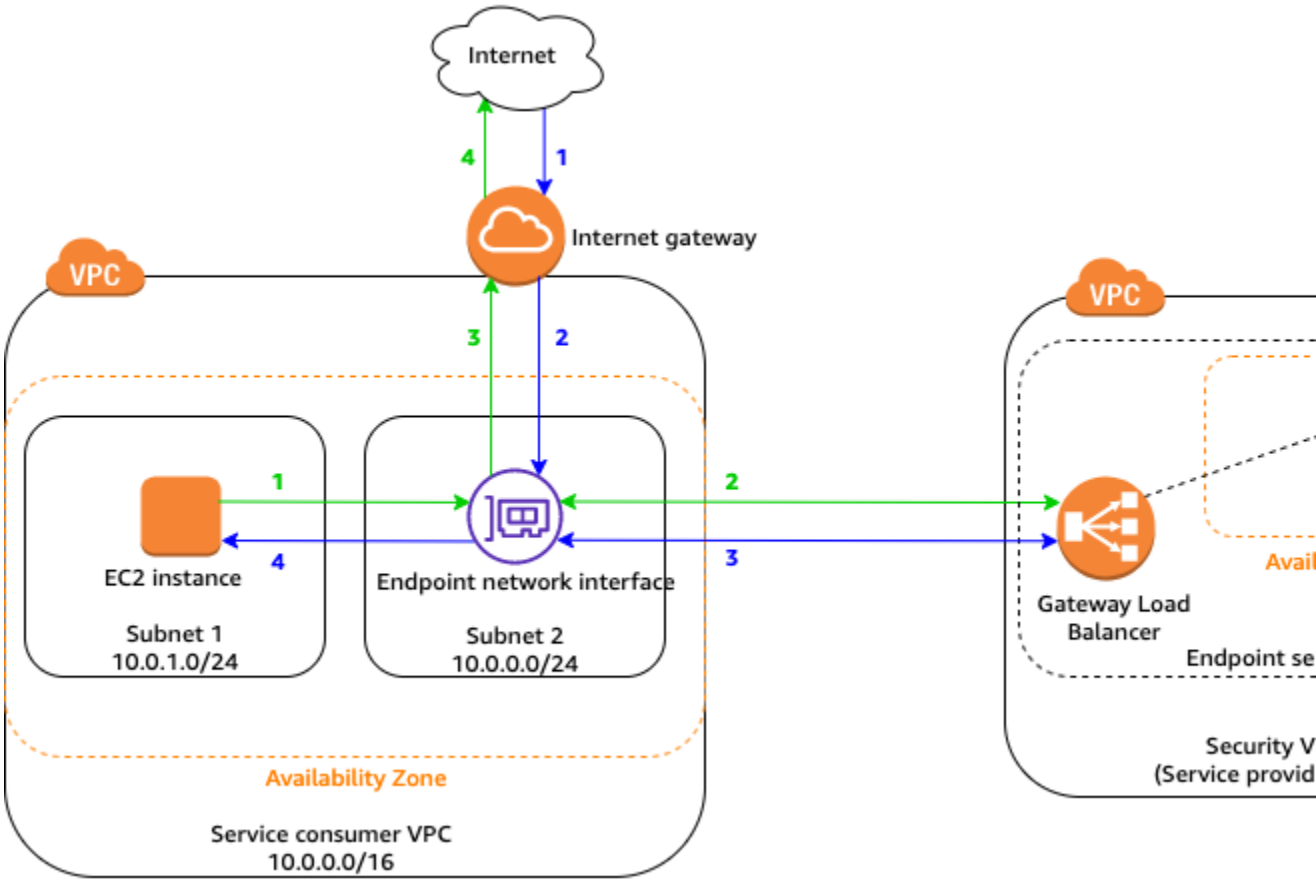
O número máximo de entradas para as listas de prefixos é equivalente ao número de entradas na tabela de rotas.

Roteamento para um endpoint do Gateway Load Balancer

Um Gateway Load Balancer permite distribuir tráfego para uma frota de dispositivos virtuais, como firewalls. Você pode configurar o balanceador de carga como um serviço criando uma configuração de serviço de VPC endpoint. Em seguida, você cria um endpoint do Gateway Load Balancer na VPC para conectá-la ao 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.

No exemplo a seguir, uma frota de dispositivos de segurança é configurada atrás de um Gateway Load Balancer na VPC de segurança. Um serviço do endpoint é configurado para o Gateway Load Balancer. O proprietário da VPC do consumidor de serviço cria um endpoint do Gateway Load Balancer na sub-rede 2 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 Gateway Load Balancer para inspeção na VPC de segurança antes de ser encaminhado para a sub-rede de destino. Da mesma forma, todo o tráfego que sai da instância do EC2 na sub-rede 1 é roteado primeiro para o endpoint do Gateway Load Balancer para inspeção na VPC de segurança antes de ser encaminhado para a Internet.



Você configura as seguintes tabelas de rotas para a VPC do consumidor de serviço.

Crie uma tabela de rotas de gateway e associe-a ao gateway de Internet. Adicione uma rota que aponte o tráfego destinado à sub-rede 1 ao endpoint do Gateway Load Balancer. Para especificar o endpoint do Gateway Load Balancer na tabela de rotas, use o ID do VPC endpoint.

Destino	Destino
10.0.0.0/16	Local
10.0.1.0/24	vpc-endpoint-id

Para a tabela de rotas da sub-rede 1, crie uma rota que aponte todo o tráfego (`0.0.0.0/0`) para o endpoint do Gateway Load Balancer. Isso garante que todo o tráfego que sai da sub-rede (destinado à Internet) seja roteado primeiro para o endpoint do Gateway Load Balancer.

Destino	Destino
10.0.0.0/16	Local
0.0.0.0/0	vpc-endpoint-id

Para a sub-rede 2, a tabela de rotas roteia o tráfego que retorna da inspeção ao destino final. Para o tráfego que se originou da Internet, a rota local assegura-se de que esteja roteada ao destino na sub-

rede 1. Para o tráfego originado da sub-rede 1, crie uma rota que roteie todo o tráfego para o gateway de Internet.

Destino	Destino
10.0.0.0/16	Local
0.0.0.0/0	igw-id

Para obter mais informações, consulte Gateway Load Balancers.

Trabalhar com tabelas de rotas

A tarefas a seguir mostram como trabalhar com tabelas de rotas.

> **Note**
>
> Quando você usa o assistente da VPC no console para criar uma VPC com um gateway, o assistente atualiza automaticamente as tabelas de rotas para usar o gateway. Se estiver usando as ferramentas de linha de comando ou a API para configurar sua VPC, você mesmo deverá atualizar as tabelas de rotas.

Tarefas

Determinar a tabela de rotas à qual uma sub-rede está associada

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 com qual tabela de rotas uma sub-rede está associada

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Sub-redes.
3. Escolha a guia Route Table para visualizar o ID da tabela e as respectivas rotas. Se for a tabela de rotas principal, o console não indicará se a associação é implícita ou explícita. Para determinar se

a associação com a tabela de rotas principal é explícita, consulte Determinar as sub-redes e/ou os gateways explicitamente associadas a uma tabela (p. 302).

Determinar as sub-redes e/ou os gateways explicitamente associadas a uma tabela

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 (p. 306).

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. Exiba a coluna Explicit subnet association (Associação de sub-rede explícita) para determinar as sub-redes explicitamente associadas.
4. Selecione a tabela de rotas desejada.
5. Escolha a guia Subnet Associations no painel de detalhes. As sub-redes associadas explicitamente à tabela estão listadas na guia. Qualquer sub-rede não associada a nenhuma tabela de rotas (e, portanto, associada implicitamente à tabela de rotas principal) também é listada.

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. Exiba a coluna Edge associations (Associações de borda) para determinar os gateways associados.
4. Selecione a tabela de rotas desejada.
5. Escolha a guia Edge Associations (Associações de borda) no painel de detalhes. Os gateways associados à tabela de rotas são listados.

Para descrever uma ou mais tabelas de rotas e exibir suas associações usando a linha de comando

- describe-route-tables (CLI da AWS)
- 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.

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 Tag de nome, insira um nome para a tabela de rotas.
5. Em VPC, escolha sua VPC.
6. (Opcional) Adicione ou remova uma tag.

   [Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

   - Em Key (Chave), insira o nome da chave.
   - Em Value (Valor), insira o valor da chave.

   [Remover uma tag] Selecione o botão de exclusão ("X") à direita da chave e do valor da tag.
7. Escolha Create (Criar).

Para criar uma tabela de rotas personalizada usando a linha de comando

- create-route-table (CLI da AWS)
- New-EC2RouteTable (AWS Tools for Windows PowerShell)

Adicionar e remover rotas de uma tabela

Você pode adicionar, excluir e modificar rotas em suas tabelas de rotas. Você só pode modificar rotas que você tenha adicionado.

Para mais informações sobre como trabalhar com rotas estáticas para uma conexão do Site-to-Site VPN, consulte Editar rotas estáticas para uma conexão do Site-to-Site VPN no Guia do usuário do AWS Site-to-Site VPN.

Para modificar ou adicionar uma rota a 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 existente, em Destination (Destino), substitua o bloco CIDR de destino ou o endereço IP único. Em Target (alvo), escolha um alvo.
6. Escolha Save routes (Salvar rotas).

Para adicionar uma rota a uma tabela de rotas usando a linha de comando

- create-route (CLI da AWS)
- New-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`.

Para substituir uma rota existente em uma tabela de rotas usando a linha de comando

- replace-route (CLI da AWS)
- Set-EC2Route (AWS Tools for Windows PowerShell)

Para excluir uma rota 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. Selecione o botão de exclusão (x) à direta da rota que deseja excluir.
5. Selecione Save routes (Salvar rotas) quando terminar.

Para excluir uma rota de uma tabela de rotas usando a linha de comando

- delete-route (CLI da AWS)
- Remove-EC2Route (AWS Tools for Windows PowerShell)

Habilitar e desabilitar a propagação de rotas

A propagação de rotas permite que um gateway privado virtual propague automaticamente rotas para as tabelas de rotas. Isso significa que você não precisa inserir manualmente rotas VPN para suas tabelas de rotas. Você pode habilitar ou desabilitar a propagação de rotas.

Para mais informações sobre as opções de roteamento VPN, 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 e selecione a tabela de rotas.
3. Selecione Actions (Ações), Edit route propagation (Editar propagação de rota).
4. Marque a caixa de seleção Propagate próxima ao gateway privado virtual e escolha Save.

Para ativar a propagação de rotas usando a linha de comando

- enable-vgw-route-propagation (CLI da AWS)
- 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 e selecione a tabela de rotas.
3. Selecione Actions (Ações), Edit route propagation (Editar propagação de rota).
4. Desmarque a caixa de seleção Propagate e escolha Save.

Para desativar a propagação de rotas usando a linha de comando

- disable-vgw-route-propagation (CLI da AWS)
- Disable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

Associar uma sub-rede a 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.

Para associar uma tabela de rotas 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 Route Tables 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 a caixa de seleção Associate para a sub-rede associada à tabela de rotas e escolha Save.

Para associar uma sub-rede a uma tabela de rotas usando a linha de comando

- associate-route-table (CLI da AWS)
- Register-EC2RouteTable (AWS Tools for Windows PowerShell)

Alterar a tabela de rotas de uma sub-rede

Você pode alterar com qual tabela de rotas uma sub-rede está associada.

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. Na lista Route Table ID (ID da tabela de rotas), selecione a nova tabela de rotas à qual associar a sub-rede e escolha Save (Salvar).

Para alterar a tabela de rotas associada a uma sub-rede usando a linha de comando

- replace-route-table-association (CLI da AWS)
- Set-EC2RouteTableAssociation (AWS Tools for Windows PowerShell)

Dissociar uma sub-rede de uma tabela de rotas

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 desassociar uma sub-rede 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 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 Associate para a sub-rede e escolha Save.

Para desassociar uma sub-rede de uma tabela de rotas usando a linha de comando

- disassociate-route-table (CLI da AWS)
- Unregister-EC2RouteTable (AWS Tools for Windows PowerShell)

Substituir a tabela de rotas principal

Você pode 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.
3. Selecione a tabela de rotas de sub-rede que deve ser a nova tabela de rotas principal e escolha Actions (Ações), Set Main Route Table (Definir tabela de rotas principal).
4. Na caixa de diálogo de confirmação, escolha OK.

Para substituir a tabela de rotas principal usando a linha de comando

- replace-route-table-association (CLI da AWS)
- 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 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 para a sub-rede e escolha Save (Salvar).

Associar um gateway a uma tabela de rotas

Você pode associar um gateway da Internet ou um gateway privado virtual com uma tabela de rotas. Para obter mais informações, consulte Tabelas de rotas do gateway (p. 288).

Para associar um gateway com 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 e selecione a tabela de rotas.
3. Escolha Actions (Ações), Edit edge associations (Editar associações de borda).
4. Escolha Gateways da Internet ou Gateways privados virtuais para exibir a lista de gateways.
5. Escolha o gateway e selecione Save (Salvar).

Como associar um gateway a uma tabela de rotas usando a CLI da AWS

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
```

Desassociar um gateway de uma tabela de rotas

Você pode desassociar um gateway da Internet ou um gateway privado virtual com uma tabela de rotas.

Para associar um gateway com 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 e selecione a tabela de rotas.
3. Escolha Actions (Ações), Edit edge associations (Editar associações de borda).
4. Em Associated gateways (Gateways Associados), escolha o botão de exclusão (x) para o gateway que deseja desassociar.
5. Escolha Save (Salvar).

Para desassociar um gateway de uma tabela de rotas usando a linha de comando

- disassociate-route-table (CLI da AWS)
- Unregister-EC2RouteTable (AWS Tools for Windows PowerShell)

Substituir e restaurar o alvo de uma rota local

Você pode alterar o alvo da rota local padrão em uma tabela de rotas de gateway (p. 288) e especificar uma interface de rede ou instância na mesma VPC que o alvo. 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 (p. 104), 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.

Não é possível substituir o alvo de uma rota local em uma tabela de rotas de sub-rede.

Para substituir o alvo por 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 e selecione a tabela de rotas.
3. Selecione Actions (Ações), Edit routes (Editar rotas).
4. Em Target (Alvo), escolha Network Interface (Interface de rede) para exibir a lista de interfaces de rede e escolha a interface de rede.

   Como alternativa, escolha Instance (Instância) para exibir a lista de instâncias e escolha a instância.
5. Escolha Save routes (Salvar rotas).

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 e selecione a tabela de rotas.

3. Selecione Actions (Ações), Edit routes (Editar rotas).
4. Em Target (Alvo), escolha local.
5. Escolha Save routes (Salvar rotas).

Como substituir o destino por uma rota local usando a CLI da AWS

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
```

Como restaurar o destino de uma rota local usando a CLI da AWS

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
```

Excluir uma tabela de rotas

Você poderá excluir uma tabela de rotas somente se não houver nenhuma sub-rede associada a ela. Você não pode excluir a tabela de rotas principal.

Para excluir 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.
3. Selecione a tabela de rotas e escolha Actions (Ações), Delete Route Table (Excluir tabela de rotas).
4. Na caixa de diálogo de confirmação, escolha Delete Route Table (Excluir tabela de rotas).

Para excluir uma tabela de rotas usando a linha de comando

- delete-route-table (CLI da AWS)
- Remove-EC2RouteTable (AWS Tools for Windows PowerShell)

Emparelhamento de VPC

Uma conexão de emparelhamento da VPC é uma conexão de redes 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 pode criar uma conexão de emparelhamento da VPC entre suas próprias VPCs, com uma VPC de outra conta da AWS ou com uma VPC em uma região diferente da AWS.

A AWS utiliza a infraestrutura existente da VPC para criar uma conexão emparelhada entre VPCs; ela não é um gateway e nem uma conexão do AWS Site-to-Site VPN e não depende de hardware físico externo. Não há um ponto único de falha de comunicação ou um gargalo de largura de banda.

Para obter mais informações sobre como trabalhar com conexões de emparelhamento de VPC e exemplos de situações em que é possível usar uma conexão de emparelhamento de VPC, consulte Guia de emparelhamento da Amazon VPC.

VPC Flow Logs

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 no Amazon CloudWatch Logs ou no Amazon S3. Após criar um log de fluxo, você poderá recuperar e visualizar seus dados no destino selecionado.

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 a taxa de transferência nem a latência da rede. É possível criar ou excluir logs de fluxo sem qualquer risco de impacto no desempenho da rede.

Tópicos

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.

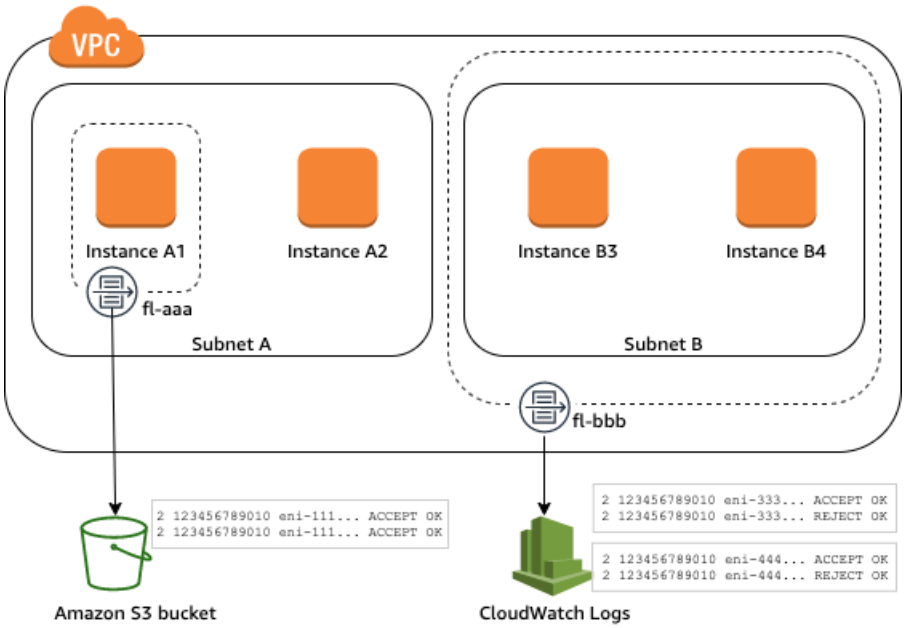
Os dados de log de fluxo para uma interface de rede monitorada são registrados como registros de log de fluxo, que são eventos de log que consistem em campos que descrevem o fluxo de tráfego. Para obter mais informações, consulte Registros de log de fluxo (p. 312).

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 (`fl-aaa`) que captura o tráfego aceito para a interface de rede da instância A1 e publica os registros de log do fluxo em um bucket do Amazon S3. Crie um segundo log de fluxo que captura todo o tráfego para a sub-rede B e publica os registros de log do fluxo no Amazon

CloudWatch Logs. O log de fluxo (`fl-bbb`) captura o tráfego para todas as interfaces de rede na sub-rede B. Não há logs de fluxo que capturam o tráfego para a interface de rede da instância A2.



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 obter mais informações, consulte Criar um log de fluxo (p. 333).

Se você iniciar mais instâncias em sua sub-rede depois de criar um log de fluxo para a sub-rede ou VPC, um novo stream de logs (para o CloudWatch Logs) ou objeto de arquivo de log (para o Amazon S3) será criado para cada nova interface de rede. Isso ocorre assim que algum tráfego de rede é registrado para essa interface de rede.

É possível 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 em uma chave e um valor opcional, ambos definidos por você. 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, você pode excluí-lo. A exclusão de um log de fluxo desabilita o serviço de log de fluxo para o recurso, e novos registros de log de fluxo não são criados nem publicados no CloudWatch Logs nem no Amazon S3. A exclusão do log de fluxo não exclui nenhum registro de log de fluxo, streams de log (para o CloudWatch Logs) nem objeto de arquivo de log (para o Amazon S3) existente para uma interface de rede. Para excluir um stream de log existente, use o console do CloudWatch Logs. Para excluir objetos de arquivo de log existentes, use o console do Amazon S3. Depois

que você exclui um log de fluxo, pode levar vários minutos para a coleta de dados se encerrar. Para obter mais informações, consulte Excluir um log de fluxo (p. 335).

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

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. Esse tempo adicional pode ser de cerca de 5 minutos para publicar no CloudWatch Logs, e cerca de 10 minutos para publicar no Amazon S3. O serviço de logs de fluxo entrega dentro desse tempo adicional da melhor maneira possível. Em alguns casos, os logs podem ser atrasados além do tempo adicional de 5 a 10 minutos mencionado anteriormente.

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 (p. 313). 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 você deve 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.

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.	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.	2
interface-id	O ID da interface de rede para a qual o tráfego é registrado.	2
srcaddr	O endereço de origem do tráfego de entrada ou o endereço IPv4 ou IPv6 da interface de rede do tráfego de saída na interface de rede. O endereço IPv4 da interface de rede sempre é o respectivo endereço IPv4 privado. Consulte também pkt-srcaddr.	2
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.	2
srcport	A porta de origem do tráfego.	2
dstport	A porta de destino do tráfego.	2
protocol	O número do protocolo IANA do tráfego. Para obter mais informações, consulte Assigned Internet Protocol Numbers.	2
packets	O número de pacotes transferidos durante o fluxo.	2
bytes	O número de bytes transferidos durante o fluxo.	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	2
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	2
action	A ação associada ao tráfego:	2

Campo	Descrição	Versão
	• ACCEPT: o tráfego registrado foi permitido por grupos de segurança e pelas Network ACLs. • REJECT: o tráfego registrado não foi permitido por grupos de segurança nem pelas Network ACLs.	
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.	2
vpc-id	O ID da VPC que contém a interface de rede para a qual o tráfego é registrado.	3
subnet-id	O ID da sub-rede que contém a interface de rede para a qual o tráfego é registrado.	3
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.	3
tcp-flags	O valor da máscara de bits para os seguintes sinalizadores TCP: • SYN: 2 • SYN-ACK: 18 • FIN: 1 • RST: 4 ACK é relatado somente quando acompanhado por SYN. 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 (p. 318).	3
type	O tipo de tráfego. Os valores possíveis são: IPv4, IPv6 e EFA. Para obter mais informações sobre o Elastic Fabric Adapter (EFA), consulte Elastic Fabric Adapter.	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 (p. 319) ou quando o endereço IP de um dispositivo 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).	3

Campo	Descrição	Versão
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 (p. 319) ou quando o endereço IP de um dispositivo 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).	3
region	A região que contém a interface de rede para a qual o tráfego é registrado.	4
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.	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.	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.	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. Os valores possíveis são: AMAZON | AMAZON_APPFLOW | AMAZON_CONNECT | API_GATEWAY | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CODEBUILD | DYNAMODB | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR | KINESIS_VIDEO_STREAMS | ROUTE53 | ROUTE53_HEALTHCHECKS | S3 | WORKSPACES_GATEWAYS .	5
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.	5
flow-direction	O sentido do fluxo em relação à interface onde o tráfego é capturado. Os valores possíveis são: ingress | egress.	5

Campo	Descrição	Versão
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 • 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)	5

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 (p. 312). Para obter informações sobre como criar logs de fluxo, consulte Trabalhar com logs de fluxo (p. 332).

Tópicos

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) para a interface de rede 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.

```
2 123456789010 eni-11111111aaaaaaaaa - - - - - - - 1431280876 1431280934 - SKIPDATA
```

Regras de grupo de segurança e network ACL

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 Network ACLs são stateless e, portanto, as respostas ao tráfego permitido estão sujeitas a regras de Network ACL.

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 stateful, o ping de resposta da sua instância é permitido. Sua Network ACL permite tráfego ICMP de entrada, mas não permite tráfego ICMP de saída. Como as Network ACLs 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 Network ACL quanto pelo security group e, por isso, obteve permissão para acessar sua instância.
- Um registro REJECT para o ping de resposta que a Network ACL 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 Network ACL 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 security group 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

O exemplo a seguir mostra um log de fluxo personalizado que captura os seguintes campos nesta ordem.

```
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 pode ajudar você a identificar a direção do tráfego como, por exemplo, qual servidor iniciou a conexão. 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. Assim, o tráfego chega ao servidor na VPC B usando eni-1111111111111111 e sai da VPC B usando eni-22222222222222222.

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:

- Não é possível ativar logs de fluxo para interfaces de rede que estejam na plataforma EC2-Classic. Isso inclui instâncias do EC2-Classic que estão vinculadas a uma VPC por meio do ClassicLink.
- Você não pode habilitar logs de fluxo para VPCs emparelhadas com a sua VPC, a menos que a VPC emparelhada esteja em sua conta.
- Depois de criar um log de fluxo, não é possível alterar a configuração dele ou o formato do registro de 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`.
- Se o tráfego for enviado de uma interface de rede e a origem não for nenhum dos endereços IP da interface de rede, o log de fluxo exibirá 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`.
- Se o tráfego for enviado para ou por uma interface de rede, os campos `srcaddr` e `dstaddr` no log de fluxo sempre exibirão o endereço IPv4 privado primário, independentemente da origem ou destino do pacote. Para capturar a origem ou o destino do pacote, crie um log de fluxo com os campos `pkt-srcaddr` e `pkt-dstaddr`.
- 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.

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 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.

Definição de preço de logs de fluxo

As cobranças de ingestão e arquivamento de dados para logs vendidos se aplicam quando você publica logs de fluxo no CloudWatch Logs ou no Amazon S3. Para obter mais informações e exemplos, consulte Definição de preço do Amazon CloudWatch.

Para monitorar as cobranças da publicação de logs de fluxo nos buckets do Amazon S3, é possível aplicar tags de alocação de custos às assinaturas do log de fluxo. Para rastrear cobranças da publicação de logs de fluxo no CloudWatch Logs, você pode aplicar tags de alocação de custos ao grupo de logs do CloudWatch Logs de destino. Depois disso, 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 mais informações, consulte Usar tags de alocação de custos no Guia do usuário do Gerenciamento de faturamento e custos da AWS.

Publicar logs de fluxo no CloudWatch Logs

Os logs de fluxo podem publicar dados de log de fluxo diretamente no Amazon CloudWatch.

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. Para obter mais informações, consulte Registros de log de fluxo (p. 312).

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.

Tópicos

Funções 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": [
    {
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Além disso, verifique se a sua função tem um relacionamento de confiança que permite que o serviço de logs de fluxo assuma a função.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Você pode atualizar uma função existente ou usar o seguinte procedimento para criar uma nova para os logs de fluxo.

Criar uma função de logs de fluxo

Como criar uma função do IAM para logs de fluxo

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Roles e depois Create Role.
3. Selecione EC2 como o serviço que usará essa função. Em Use case (Caso de uso), selecione EC2. Escolha Próximo: Permissões.
4. Na página Attach permissions policies (Anexar políticas de permissões), selecione Next: Tags (Próximo: tags) e, se desejar, adicione tags. Selecione Next: Review (Próximo: revisão).
5. Insira um nome para a sua função (por exemplo, `Flow-Logs-Role`), e você também pode fornecer uma descrição. Selecione Create role (Criar função).
6. Selecione o nome de sua função. Em Permissions (Permissões), selecione Add inline policy (Adicionar política em linha) e JSON.
7. Copie a primeira política de Funções do IAM para publicar logs de fluxo no CloudWatch Logs (p. 322) e cole-a na janela. Escolha Review policy (Revisar política).
8. Insira um nome para a política e selecione Create policy (Criar política).
9. Selecione o nome de sua função. Em Trust relationships (Relacionamentos de confiança), selecione Edit trust relationship (Editar relacionamento de confiança). No documento da política existente, altere o serviço de `ec2.amazonaws.com` para `vpc-flow-logs.amazonaws.com`. Escolha Update Trust Policy.
10. Na página Summary (Resumo), anote o ARN da sua função. Você precisa desse ARN para criar o log de fluxo.

Permissões para que os usuários do IAM passem uma função

Os usuários também devem ter permissões para usar a ação `iam:PassRole` para a função do IAM associada ao log de fluxo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Action": ["iam:PassRole"],
      "Resource": "arn:aws:iam::account-id:role/flow-log-role-name"
    }
  ]
}
```

Criar um log de fluxo que publica no CloudWatch Logs

É possível criar logs de fluxos para suas VPCs, sub-redes ou interfaces de rede. Se executar essas etapas como um usuário do IAM, verifique se você tem permissões para usar a ação `iam:PassRole`. Para obter mais informações, consulte Permissões para que os usuários do IAM passem uma função (p. 323).

Pré-requisito

Crie o grupo de logs de destino. Abra a página Grupos de log no console do CloudWatch e escolha Create log group (Criar grupo de log) . Digite um nome para o grupo de log e selecione Create (Criar).

Para criar um log de fluxo para uma interface de rede usando o 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 as caixas de seleção para uma ou mais interfaces de rede e escolha Actions (Ações), Create flow log (Criar log de fluxo).
4. Em Filter (Filtrar), especifique o tipo de tráfego a ser registado. Selecione All (Todos) para registrar o tráfego aceito e rejeitado, Rejected (Rejeitado) para registrar somente o tráfego rejeitado ou Accepted (Aceito) para registrar somente o tráfego aceito.
5. 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.
6. Para Destination (Destino), escolha Send to CloudWatch Logs (Enviar para o CloudWatch Logs).
7. Para Destination log group (Grupo de log de destino), escolha o nome do grupo de log de destino que você criou.
8. Em IAM role (Função do IAM), especifique o nome da função que tem as permissões para publicar logs no CloudWatch Logs.
9. Para Log record format (Formato de registro de log) , selecione o formato para o registro de log de fluxo.
   - Para usar o formato padrão, escolha AWS default format (Formato padrão da AWS).
   - Para usar um formato personalizado, escolha Custom format (Formato personalizado) e, em seguida, selecione os campos de Log format (Formato de log) .
   - Para criar um log de fluxo personalizado que inclua os campos padrão, escolha AWS default format (Formato padrão da AWS), copie os campos em Format preview (Visualização do formato), escolha Custom format (Formato personalizado) e cole os campos na caixa de texto.
10. (Opcional) Escolha Add new tag (Adicionar nova tag) para aplicar tags ao log de fluxo.
11. Selecione Create flow log (Criar log de fluxo).

Para criar um log de fluxo para uma VPC ou 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 Your VPCs (Suas VPCs) ou Subnets (Sub-redes).
3. Selecione a caixa de seleção para uma ou mais VPCs ou sub-redes e escolha Actions (Ações), Create flow log (Criar log de fluxo).

4. Em Filter (Filtrar), especifique o tipo de tráfego a ser registado. Selecione All (Todos) para registrar o tráfego aceito e rejeitado, Rejected (Rejeitado) para registrar somente o tráfego rejeitado ou Accepted (Aceito) para registrar somente o tráfego aceito.
5. 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.
6. Para Destination (Destino), escolha Send to CloudWatch Logs (Enviar para o CloudWatch Logs).
7. Para Destination log group (Grupo de log de destino), escolha o nome do grupo de log de destino que você criou.
8. Em IAM role (Função do IAM), especifique o nome da função que tem as permissões para publicar logs no CloudWatch Logs.
9. Para Log record format (Formato de registro de log) , selecione o formato para o registro de log de fluxo.
   - Para usar o formato padrão, escolha AWS default format (Formato padrão da AWS).
   - Para usar um formato personalizado, escolha Custom format (Formato personalizado) e, em seguida, selecione os campos de Log format (Formato de log) .
   - Para criar um log de fluxo personalizado que inclua os campos padrão, escolha AWS default format (Formato padrão da AWS), copie os campos em Format preview (Visualização do formato), escolha Custom format (Formato personalizado) e cole os campos na caixa de texto.
10. (Opcional) Escolha Add new tag (Adicionar nova tag) para aplicar tags ao log de fluxo.
11. Selecione Create flow log (Criar log de fluxo).

Para criar um log de fluxo usando a linha de comando

Use um dos seguintes comandos.

- create-flow-logs (CLI da AWS)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowLogs (API de consulta do Amazon EC2)

A CLI da AWS demonstrativa a seguir cria um log de fluxo que captura todo o tráfego aceito para a sub-rede `subnet-1a2b3c4d`. Os logs de fluxo são entregues a um grupo de logs no CloudWatch Logs chamado `my-flow-logs`, na conta 123456789101, usando a função do IAM `publishFlowLogs`.

```
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
```

Processar registros de log de fluxo no CloudWatch Logs

É possível trabalhar com registro de log de fluxo do mesmo modo que você trabalharia com outros eventos de coletados pelo CloudWatch Logs. Para obter mais informações sobre monitoramento de dados de log e filtros de métricas, consulte Pesquisar e filtrar dados de log no Guia do usuário do Amazon CloudWatch.

Exemplo: criar um filtro de métricas no CloudWatch e um alarme para um log de fluxo

Neste exemplo, você tem 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.

Para 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, selecione Logs.
3. Escolha o valor associado de Metric Filters (Filtros de métrica) para o grupo de logs do log de fluxo e selecione Add Metric Filter (Adicionar filtro de métrica).
4. Em Filter Pattern (Padrão de filtro), insira o seguinte.

```
[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 de sua interface de rede. (Optional) Para visualizar as linhas de dados de log que correspondem ao padrão do filtro, selecione Test Pattern (Padrão de teste). Quando estiver pronto, escolha Assign Metric.
6. Forneça o namespace e o nome da métrica e verifique se o valor da métrica está definido como 1. Quando concluir, escolha Create Filter.
7. No painel de navegação, escolha Alarms, Create Alarm.
8. Na seção Custom Metrics, escolha o namespace do filtro de métricas que você criou.

   Pode levar alguns minutos para uma nova métrica ser exibida no console.
9. Selecione o nome da métrica que você criou e Next (Próximo).
10. Digite um nome e uma descrição para o alarme. Nos campos is (é), selecione >= e insira 10. No campo for (para), deixe o padrão 1 para os períodos consecutivos.
11. Em Period (Período), selecione 1 Hour (1 hora). Em Statistic (Estatística), selecione Sum (Soma). A estatística `Sum` é uma garantia de que você está capturando o número total de pontos de dados do período especificado.
12. Na seção Actions (Ações), você pode optar por enviar um notificação para uma lista existente. Ou, você pode criar uma nova lista e inserir os endereços de e-mail que deverão receber uma notificação quando o alarme for acionado. Quando concluir, escolha Create Alarm:

Publicar logs de fluxo no Amazon S3

Os logs de fluxo podem publicar dados de log de fluxo no Amazon S3.

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 obter mais informações, consulte Registros de log de fluxo (p. 312).

Para criar um bucket do Amazon S3 para uso com logs de fluxo, consulte Criar um bucket no Guia de conceitos básicos do Amazon Simple Storage Service.

Tópicos

- Criar um log de fluxo para publicação no Amazon S3 (p. 330)
- Processar registros de log de fluxo no Amazon S3 (p. 332)

Arquivos de log de fluxo

Os logs de fluxo coletam registros de log de fluxo, os consolidam em arquivos de log e publicam os arquivos de log no bucket do Amazon S3; em intervalos de 5 minutos. Cada arquivo de log contém os registros de log de fluxo para o tráfego de IP registrado nos últimos cinco minutos.

O tamanho máximo de um arquivo de log é de 75 MB. Se o arquivo de log atingir o limite de tamanho no período de 5 minutos, o log de fluxo deixará de adicionar registros de log de fluxo. Depois, ele publicará o log de fluxo no bucket do Amazon S3 e criará um novo arquivo de log.

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 e pela data em que são criados. A estrutura de pasta do bucket usa o seguinte formato.

```
bucket_ARN/optional_folder/AWSLogs/aws_account_id/
vpcflowlogs/region/year/month/day/log_file_name.log.gz
```

Da mesma forma, o nome do arquivo de log será determinado pelo ID do log de fluxo, pela região e pela data e a hora em que foi criada pelo serviço de logs de fluxo. Os nomes de arquivo usam o seguinte formato. O time stamp usa o formato `YYYYMMDDTHHmmZ`.

```
aws_account_id_vpcflowlogs_region_flow_log_id_timestamp_hash.log.gz
```

Por exemplo, veja a seguir a estrutura de pasta e o nome de arquivo de um arquivo de log para um log de fluxo criado pela conta da AWS `123456789012`, para um recurso na região `us-east-1`, em `June 20, 2018` às `16:20 UTC`. Ele inclui os registros de log de fluxo com um tempo de término entre `16:20:00` e `16:24:59`.

```
arn:aws:s3:::my-flow-log-bucket/AWSLogs/123456789012/
vpcflowlogs/us-east-1/2018/06/20/123456789012_vpcflowlogs_us-
east-1_fl-1234abcd_20180620T1620Z_fe123456.log.gz
```

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. Isso 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.

Política do IAM para entidades principais do IAM que publicam logs de fluxo no Amazon S3

Uma entidade principal do IAM na sua conta, como um usuário do IAM, deve ter permissões suficientes para publicar logs de fluxo no bucket do Amazon S3. Isso inclui permissões para trabalhar com ações `logs:` específicas para criar e publicar os logs de fluxo. A política do IAM deve incluir as permissões a seguir.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Action": [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
        ],
      "Resource": "*"
    }
  ]
}
```

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.

A política de bucket a seguir oferece ao log de fluxo permissão para publicar logs nele. Se o bucket já tiver uma política com as permissões a seguir, a política será mantida como está. Recomendamos conceder essas permissões para o principal do serviço de entrega de log em vez de ARNs individuais da conta da AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/optional_folder/AWSLogs/account_id/*",
            "Condition": {"StringEquals": {"s3:x-amz-acl": "bucket-owner-full-control"}}
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::bucket_name"
        }
    ]
}
```

Se o usuário que cria o log de fluxo for o proprietário do bucket, tiver permissões `PutBucketPolicy` para o bucket e o bucket não tiver uma política com permissões de entrega de log suficientes, anexaremos automaticamente a política anterior ao bucket. Esta política substitui qualquer política existente anexada ao bucket.

Se o usuário que cria um evento de fluxo não possui o bucket nem tem as permissões `GetBucketPolicy` e `PutBucketPolicy` para o bucket, ocorre uma falha na criação do log de fluxo. Nesse caso, o proprietário do bucket deve adicionar manualmente as políticas acima ao bucket e especificar o ID de conta da AWS do criador do log de fluxo. Para obter mais informações, consulte Como excluir um bucket do S3? no Guia do usuário do console do Amazon Simple Storage Service. Se o bucket recebe logs de fluxo de várias contas, adicione uma entrada de elemento `Resource` à declaração de política `AWSLogDeliveryWrite` para cada conta. Por exemplo, a política de bucket a seguir permite que as contas da AWS `123123123123` e `456456456456` publiquem logs de fluxo na pasta chamada `flow-logs` de um bucket chamado `log-bucket`.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": [
             "arn:aws:s3:::log-bucket/flow-logs/AWSLogs/123123123123/*",
             "arn:aws:s3:::log-bucket/flow-logs/AWSLogs/456456456456/*"
             ],
            "Condition": {"StringEquals": {"s3:x-amz-acl": "bucket-owner-full-control"}}
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::log-bucket"
        }
    ]
}
```

Política de chaves de CMK obrigatórias para uso com SSE-KMS

Você pode proteger os dados em seu bucket do Amazon S3 habilitando a criptografia no lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) ou a criptografia do lado do servidor com Customer Master Keys (CMKs – chaves mestras do cliente) armazenadas no AWS Key Management Service (SSE-KMS). Para obter mais informações, consulte Proteger dados usando criptografia do lado do servidor no Guia do usuário do Amazon S3.

Com o SSE-KMS, você pode usar uma CMK gerenciada pela AWS ou uma CMK gerenciada pelo cliente. Com uma CMK gerenciada pela AWS, você não pode usar a entrega entre contas. Os logs de fluxo são entregues a partir da conta de entrega de log, portanto, você deve conceder acesso para entrega entre contas. Para conceder acesso entre contas ao bucket do S3, use uma CMK gerenciada pelo cliente e especifique o Nome de recurso da Amazon (ARN) da CMK gerenciada pelo cliente ao habilitar a criptografia de bucket. Para obter mais informações, consulte Especificar criptografia no lado do servidor com o AWS KMS no Guia do usuário do Amazon S3 .

Quando você usa o SSE-KMS com uma CMK gerenciada pelo cliente, você deve adicionar o seguinte à política de chaves da CMK (não à política de bucket para o bucket do S3), para que os logs de fluxo da VPC possam gravar no bucket do S3.

```
{
    "Sid": "Allow VPC Flow Logs to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
        ]
    },
   "Action": [
       "kms:Encrypt",
       "kms:Decrypt",
       "kms:ReEncrypt*",
       "kms:GenerateDataKey*",
       "kms:DescribeKey"
    ],
    "Resource": "*"
```

```
}
```

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 desenvolvedor do Amazon Simple Storage Service.

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 VPCs, sub-redes ou interfaces de rede.

Para criar um log de fluxo para uma interface de rede usando o 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 uma ou mais interfaces de rede e escolha Actions (Ações), Create flow log (Criar log de fluxo).
4. Em Filter (Filtro), especifique o tipo de dados de tráfego de IP para registrar 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.
5. 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.
6. Em Destination (Destino), escolha Send to an Amazon S3 bucket (Enviar para um bucket do Amazon S3).
7. Para S3 bucket ARN (ARN do bucket do S3), especifique o nome de recurso da Amazon (ARN) de um bucket existente do Amazon S3. Você pode incluir uma subpasta no ARN do bucket. O bucket não pode usar `AWSLogs` como um nome de subpasta, pois se trata de um termo reservado.

   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/
   ```

   Se você for o proprietário do bucket, criamos automaticamente uma política de recurso e a anexamos ao bucket. Para obter mais informações, consulte Permissões do bucket do Amazon S3 para logs de fluxo (p. 328).
8. Em Format (Formato), especifique o formato do registro de log de fluxo.

   - Para usar o formato de registro de log de fluxo padrão, escolha AWS default format (Formato padrão da AWS).
   - Para criar um formato personalizado, escolha Custom format (Formato personalizado). Em Log format (Formato de log), escolha os campos a serem incluídos no registro de log de fluxo.

     Tip

     Para criar um log de fluxo personalizado que inclua campos de formato padrão, primeiro escolha AWS default format (Formato padrão da AWS), copie os campos em Format preview (Visualização do formato), escolha Custom format (Formato personalizado) e cole os campos na caixa de texto.

9. (Opcional) Escolha Add Tag (Adicionar tag) para aplicar tags ao log de fluxo.
10. Escolha Criar.

Para criar um log de fluxo para uma VPC ou 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, selecione Your VPCs (Suas VPCs) ou Subnets (Sub-redes).
3. Selecione uma ou mais VPCs ou sub-redes e escolha Actions (Ações), Create flow log (Criar log de fluxo).
4. Em Filter (Filtro), especifique o tipo de dados de tráfego de IP para registrar 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.
5. 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.
6. Em Destination (Destino), escolha Send to an Amazon S3 bucket (Enviar para um bucket do Amazon S3).
7. Para S3 bucket ARN (ARN do bucket do S3), especifique o nome de recurso da Amazon (ARN) de um bucket existente do Amazon S3. Você pode incluir uma subpasta no ARN do bucket. O bucket não pode usar `AWSLogs` como um nome de subpasta, pois se trata de um termo reservado.

   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/
   ```

   Se você for o proprietário do bucket, criamos automaticamente uma política de recurso e a anexamos ao bucket. Para obter mais informações, consulte Permissões do bucket do Amazon S3 para logs de fluxo (p. 328).
8. Em Format (Formato), especifique o formato do registro de log de fluxo.
   - Para usar o formato de registro de log de fluxo padrão, escolha AWS default format (Formato padrão da AWS).
   - Para criar um formato personalizado, escolha Custom format (Formato personalizado). Em Log format (Formato de log), escolha os campos a serem incluídos no registro de log de fluxo.
9. (Opcional) Escolha Add Tag (Adicionar tag) para aplicar tags ao log de fluxo.
10. Escolha Criar.

Como criar um log de fluxo publicado no Amazon S3 usando uma ferramenta de linha de comando

Use um dos seguintes comandos.

- create-flow-logs (CLI da AWS)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowLogs (API de consulta do Amazon EC2)

A CLI da AWS demonstrativa a seguir cria um log de fluxo que captura todo o tráfego da VPC `vpc-00112233344556677` e fornece os logs de fluxo para um bucket do Amazon S3 chamado `flow-log-bucket`. 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/my-custom-flow-logs/ --log-format '${version} ${vpc-id} ${subnet-id} ${instance-
```

```
id} ${srcaddr} ${dstaddr} ${srcport} ${dstport} ${protocol} ${tcp-flags} ${type} ${pkt-
srcaddr} ${pkt-dstaddr}'
```

Processar registros de log de fluxo no Amazon S3

Os arquivos de log são compactados. Se você abrir os arquivos de log usando o console do Amazon S3, eles serão descompactados, e os registros de log de fluxo serão exibidos. Se você baixar os arquivos, será necessário descompactá-los para visualizar os registros de log de fluxo.

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 Guia do usuário do Amazon Athena.

Trabalhar com logs de fluxo

É possível trabalhar com logs de fluxo usando os consoles do Amazon EC2, da Amazon VPC, do CloudWatch e do Amazon S3.

Tarefas

Controlar o uso de logs de fluxo

Por padrão, os usuários do IAM não têm permissão para trabalhar com logs de fluxo. É possível criar uma política de usuário do IAM que conceda permissões aos usuários para criar, descrever e excluir logs de fluxo. Para obter mais informações, consulte Conceder aos usuários do IAM as permissões necessárias para os recursos do Amazon EC2 na Referência de API do Amazon EC2.

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": "*"
    }
  ]
}
```

Algumas configurações adicionais de funções e permissões do IAM são necessárias, dependendo se você está publicando no CloudWatch Logs ou no Amazon S3. Para obter mais informações, consulte Publicar logs de fluxo no CloudWatch Logs (p. 322) e Publicar logs de fluxo no Amazon S3 (p. 326).

Criar um log de fluxo

É possível criar logs de fluxos para suas VPCs, sub-redes ou interfaces de rede. Os logs de fluxo podem publicar dados no CloudWatch Logs ou no Amazon S3.

Para obter mais informações, consulte Criar um log de fluxo que publica no CloudWatch Logs (p. 324) e Criar um log de fluxo para publicação no Amazon S3 (p. 330).

Visualizar logs de fluxo

É possível visualizar informações sobre os logs de fluxo no console do Amazon EC2 e da Amazon VPC por meio da visualização da guia Flow Logs (Logs de fluxo) correspondente a um recurso específico. Ao selecionar o recurso, todos os logs de fluxo correspondentes são listados. As informações exibidas incluem o ID do log de fluxo, a configuração do log de fluxo e o status do log de fluxo.

Para visualizar informações sobre os logs de fluxos de suas interfaces de rede

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 e Flow Logs (Logs de fluxo). As informações sobre os logs de fluxo são exibidas nessa guia. A coluna Destination type (Tipo de destino) indica o destino no qual os logs de fluxo são publicados.

Para visualizar informações sobre os logs de fluxo de suas VPCs ou sub-redes

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Your VPCs (Suas VPCs) ou Subnets (Sub-redes).
3. Selecione sua VPC ou sub-rede e Flow Logs (Logs de fluxo). As informações sobre os logs de fluxo são exibidas nessa guia. A coluna Destination type (Tipo de destino) indica o destino no qual os logs de fluxo são publicados.

Adicionar ou remover tags para logs de fluxo

É possível adicionar ou remover tags para um log de fluxo nos consoles do Amazon EC2 e da Amazon VPC.

Como adicionar ou remover tags para um log de fluxo para uma interface de rede

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 e Flow Logs (Logs de fluxo).
4. Escolha Manage tags (Gerenciar tags) para o log de fluxo necessário.
5. Para adicionar uma nova tag, escolha Criar tag. Para remover uma tag, escolha o botão Excluir (x).
6. Escolha Save (Salvar).

Como adicionar ou remover tags para um log de fluxo para uma VPC ou sub-rede

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

2. No painel de navegação, selecione Your VPCs (Suas VPCs) ou Subnets (Sub-redes).
3. Selecione sua VPC ou sub-rede e Flow Logs (Logs de fluxo).
4. Selecione o log de fluxo e escolha Actions (Ações), Add/Edit Tags (Adicionar/Editar tags).
5. Para adicionar uma nova tag, escolha Criar tag. Para remover uma tag, escolha o botão Excluir (x).
6. Escolha Save (Salvar).

Visualizar registros de log de fluxo

É possível visualizar registros de log de fluxo usando o console do CloudWatch Logs ou do Amazon S3, dependendo do tipo de destino selecionado. Depois que o log de fluxo é criado, pode levar alguns minutos para ele ficar visível no console.

Como 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 e o grupo de logs que contém o seu log de fluxo. É exibida uma lista de streams de logs para cada interface de rede.
3. Selecione o fluxo de logs que contém o ID da interface de rede para a qual os registros de log de fluxo serão visualizados. Para obter mais informações, consulte Registros de log de fluxo (p. 312).

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. Em Bucket name (Nome do bucket), selecione o bucket no qual os logs de fluxo são publicados.
3. Em Name (Nome), marque a caixa de seleção ao lado do arquivo de log. No painel de visão geral do objeto, selecione Download (Baixar).

Pesquisar registros de log de fluxo

É possível pesquisar os registros de log de fluxo publicados no CloudWatch Logs usando o console do CloudWatch Logs. Você pode usar filtros de métrica 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 e o grupo de logs que contém seu log de fluxo. É exibida uma lista de streams de logs para cada interface de rede.
3. Selecione o fluxo de log individual se souber a interface de rede que está pesquisando. Como alternativa, escolha Pesquisar grupo de logs para pesquisar todo o 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 Filter events (Filtrar eventos), insira a string a seguir. Isso pressupõe que o registro de log de fluxo usa o formato padrão (p. 312).

```
[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]
```

Excluir um log de fluxo

É possível excluir um log de fluxo usando os consoles do Amazon EC2 e da Amazon VPC.

Esses procedimentos desativam o serviço de log de fluxo de um recurso. A exclusão de um log de fluxo não exclui os streams de log existentes do CloudWatch Logs e arquivos de log do Amazon S3. Os dados de log de fluxo existentes devem ser excluídos por meio do respectivo console de serviço. Além disso, a exclusão de um log de fluxo que publica no Amazon S3 não remove as políticas de bucket e as listas de controle de acesso (ACLs).

Para excluir um log de fluxo de uma interface de rede

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Interfaces de rede e selecione a interface de rede.
3. Selecione Flow Logs (Logs de fluxo) e, em seguida, selecione o botão de exclusão (uma cruz) para excluir o log de fluxo.
4. Na caixa de diálogo de confirmação, escolha Yes, Delete.

Para excluir um log de fluxo para uma VPC ou uma sub-rede

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Your VPCs (Suas VPCs) ou Subnets (Sub-redes) e, em seguida, selecione o recurso.
3. Selecione Flow Logs (Logs de fluxo) e, em seguida, selecione o botão de exclusão (uma cruz) para excluir o log de fluxo.
4. Na caixa de diálogo de confirmação, escolha Yes, Delete.

Visão geral da API e da CLI

Você pode executar as tarefas descritas nesta página 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 Acessar a Amazon VPC (p. 1).

Criar um log de fluxo

- create-flow-logs (CLI da AWS)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)
- CreateFlowLogs (API de consulta do Amazon EC2)

Descrever seus logs de fluxo

- describe-flow-logs (CLI da AWS)
- Get-EC2FlowLog (AWS Tools for Windows PowerShell)
- DescribeFlowLogs (API de consulta do Amazon EC2)

Visualizar seus registros de log de fluxo (eventos de log)

- get-log-events (CLI da AWS)
- Get-CWLLogEvent (AWS Tools for Windows PowerShell)
- GetLogEvents (API do CloudWatch)

Excluir um log de fluxo

- delete-flow-logs (CLI da AWS)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)
- DeleteFlowLogs (API de consulta do Amazon EC2)

Como 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.

Você pode simplificar e automatizar a integração dos seus 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 sua VPC.

O modelo do CloudFormation cria os seguintes recursos:

- 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 (p. 338).
- 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.

Requisitos

- Você deve selecionar uma região que ofereça suporte ao AWS Lambda e ao Amazon Athena.
- Os buckets do Amazon S3 devem estar na região selecionada.

Definição de preços

Você incorre em cobranças padrão do Amazon Athena pelas consultas feitas. Você incorre em cobranças padrão do AWS Lambda pela 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).

Tarefas

- Como gerar o modelo do CloudFormation usando o console (p. 337)
- Como gerar o modelo do CloudFormation usando a AWS CLI (p. 337)
- Como realizar uma consulta predefinida (p. 338)

Como 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.

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.

Como 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
```

Como realizar uma consulta predefinida

O modelo 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. No painel Workgroups (Grupos de trabalho), selecione o grupo de trabalho criado pelo modelo do CloudFormation.
2. Selecione uma das consultas predefinidas (p. 338), modifique os parâmetros conforme necessário e, então, execute-a.
3. Abra o console do Amazon S3. Navegue até o bucket que você especificou para os resultados da consulta e visualize os resultados da consulta.

Consultas predefinidas

A seguir estão as consultas nomeadas do Athena fornecidas pelo modelo gerado do CloudFormation:

- VPCFlowLogsAcceptedTraffic: as conexões TCP que foram permitidas com base nos seus grupos de segurança e ACLs de rede.
- VPCFlowLogsAdminportTraffic: o tráfego registrado em portas administrativas de aplicações Web.
- 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.

Solução de problemas de logs de fluxo da VPC

Veja a seguir os possíveis problemas que você pode ter ao trabalhar com logs de fluxo.

Problemas

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. Para obter mais informações, consulte Visualizar logs de fluxo (p. 333). 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 podem ser exibidos:

- `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 Guia 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 obter mais informações, consulte Funções do IAM para publicar logs de fluxo no CloudWatch Logs (p. 322).

- `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 e o console da Amazon VPC ou do Amazon EC2 exibe esse log como `Active`. No entanto, não é possível ver nenhum stream de log no CloudWatch Logs nem arquivos de log no bucket do Amazon S3.

Causa

A causa pode ser uma das seguintes:

- A criação do log de fluxo ainda está em processo. Em alguns casos, pode demorar 10 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

Recebe um erro `Access Denied for LogDestination` ou `LogDestinationNotFoundException` quando tenta criar um log de fluxo.

Causa

É possível receber esse erro na criação de um log de fluxo que publique dados em um bucket do Amazon S3. Esse erro indica que o bucket do S3 especificado não pôde ser encontrado ou que há um problema com a política de bucket.

Solução

Faça uma das coisas a seguir:

- Verifique se você especificou o ARN para um bucket do S3 existente e se o ARN está no formato correto.
- Se não possuir o bucket do S3, verifique se a bucket policy (política de bucket) (p. 328) tem permissões suficientes para publicar logs nele. Na política de bucket, verifique o ID da conta e o nome do bucket.

Exceder o limite de políticas de buckets do Amazon S3

Problema

Você obtém o seguinte erro ao tentar criar um log de fluxo: `LogDestinationPermissionIssueException`.

Causa

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

Faça uma das coisas a seguir:

- 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.

Conexões VPN

É possível conectar sua Amazon 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 do Site-to-Site VPN, um gateway privado virtual ou um gateway de trânsito fornece dois VPN endpoints (túneis) para o failover automático. Configure seu dispositivo de gateway do cliente no lado remoto da conexão do Site-to-Site VPN. Para mais informações, consulte o Guia do usuário do AWS Site-to-Site VPN.
AWS Client VPN	O AWS Client VPN é um serviço de VPN gerenciado no cliente que permite que você acesse de forma segura os recursos da AWS na sua rede local. Com ele, 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 possam acessar recursos na AWS ou no local de qualquer lugar usando uma VPN cliente do tipo OpenVPN-based . Para obter mais informações, consulte o Guia do administrador da AWS Client VPN.
AWS VPN CloudHub	Havendo mais de uma rede remota (por exemplo, várias filiais), é possível a criação de diversas conexões do AWS Site-to-Site VPN por meio do gateway privado virtual, permitindo a comunicação entre as redes. Para mais informações, consulte Garantir a comunicação segura entre os sites usando o VPN CloudHub no Guia do usuário do AWS Site-to-Site VPN.
Dispositivo VPN de software terceirizado	Crie uma conexão VPN para a rede remota usando uma instância do Amazon EC2 na VPC que estiver executando um dispositivo VPN de software de terceiros. A AWS não fornece nem mantém dispositivos VPN de software de terceiros, contudo, é possível escolher um dentre os diversos produtos fornecidos por parceiros e comunidades de código aberto. Encontre dispositivos VPN de software de terceiros no AWS Marketplace.

Também é possível usar o AWS Direct Connect para criar uma conexão privada dedicada de uma rede remota para a VPC. Combine essa conexão com o AWS Site-to-Site VPN para criar uma conexão criptografada por IPsec. Para obter mais informações, consulte O que é o AWS Direct Connect? no Guia do usuário do AWS Direct Connect.

AWS PrivateLink e VPC endpoints

O AWS PrivateLink estabelece conectividade privada entre virtual private clouds (VPCs) e serviços hospedados na AWS ou on-premises, sem expor dados na Internet.

Um VPC endpoint permite que você conecte de forma privada a VPC aos serviços da AWS compatíveis e aos serviços do VPC endpoint desenvolvidos pelo AWS PrivateLink sem exigir um gateway da Internet, um dispositivo NAT, uma conexão VPN ou uma conexão do AWS Direct Connect. As instâncias na sua VPC não exigem que endereços IP públicos se comuniquem com recursos no serviço. O tráfego entre a sua VPC e os outros serviços não deixa a rede da Amazon.

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

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 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, consulte Grupos de regras no 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 Guida do desenvolvedor do AWS WAF, AWS Firewall Manager e do AWS Shield Advanced.

Cotas da Amazon VPC

As tabelas a seguir listam as cotas, anteriormente denominadas limites, para os recursos da Amazon VPC por região para sua conta da AWS. Salvo indicação em contrário, é possível solicitar um aumento para essas cotas. Para algumas dessas cotas, será possível visualizar a cota atual usando a página Limits (Limites) do console do Amazon EC2.

Se solicitar um aumento de cota que seja aplicável por recurso, aumentaremos a cota para todos os recursos na Região.

VPC e sub-redes

Recurso	Padrã	Comentários
VPCs por região	5	A cota de gateways de Internet por Região está diretamente correlacionada a essa. Se essa cota for aumentada, a cota em gateways da Internet por Região será aumentada no mesmo valor. Você pode ter centenas de VPCs por região para atender às suas necessidades, mesmo que a cota padrão seja de 5 VPCs por região.
Sub-redes por VPC	200	–
Blocos CIDR IPv4 por VPC	5	Esse bloco CIDR primário e todos os blocos CIDR secundários são contabilizados de acordo com essa cota. Essa cota pode ser aumentada até um número máximo de 50.
Blocos CIDR IPv6 por VPC	1	Essa cota não pode ser aumentada.

DNS

Cada instância do EC2 limita o número de pacotes que podem ser enviados para o Amazon Route 53 Resolver (especificamente endereços .2, como 10.0.0.2 e 169.254.169.253), até no máximo 1024 pacotes por segundo por interface de rede. Essa cota não pode ser aumentada. O número de consultas DNS por segundo ao qual o resolvedor do Amazon Route 53 oferece suporte 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 dimensionável, consulte o whitepaper Hybrid Cloud DNS Solutions for Amazon VPC.

Endereços IP elásticos (IPv4)

Recurso	Padrão	Comentários
Endereços IP elásticos por região	5	Essa é a cota para o número de endereços IP elásticos para uso na EC2-VPC. Para

Recurso	Padrão	Comentários
		endereços IP elásticos para uso no EC2-Classic, consulte Endpoints e cotas do Amazon Elastic Compute Cloud na Referência geral da Amazon Web Services. Essa cota se aplica a VPCs individuais da conta da AWS e VPCs compartilhadas.

Gateways

Recurso	Padrão	Comentários
Gateways do cliente por região	–	Para mais informações, consulte Cotas do Site-to-Site VPN no Guia do usuário do AWS Site-to-Site VPN.
Gateways da Internet somente de saída por região	5	Essa cota está diretamente relacionada à cota de VPCs por região. Para aumentá-la, aumente a cota de VPCs por região. Você pode anexar apenas um gateway da internet somente de saída a uma VPC de cada vez.
Gateways da Internet por região	5	Essa cota está diretamente relacionada à cota de VPCs por região. Para aumentá-la, aumente a cota de VPCs por região. Apenas um gateway da internet pode ser associado a uma VPC de cada vez.
Gateways de NAT por zona de disponibilidade	5	Um gateway NAT nas contagens de estado `pending`, `active` ou `deleting` é contabilizado na sua cota.
Gateways privados virtuais por região	–	Para mais informações, consulte Cotas do Site-to-Site VPN no Guia do usuário do AWS Site-to-Site VPN.
Gateways de operadora por VPC	1	

Listas de prefixos gerenciadas pelo cliente

Recurso	Padrão	Comentários
Listas de prefixos por região	100	–
Versões por lista de prefixos	1.000	No cenário em que 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 e permaneça dentro da cota.
Número máximo de entradas por lista de prefixos	1.000	

Recurso	Padrão	Comentários
Referências a uma lista de prefixos por tipo de recurso	5.000	Essa cota se aplica de acordo com o tipo de recurso que pode fazer referência a uma lista de prefixos. Por exemplo, você pode ter 5.000 referências a uma lista de prefixos em todos os grupos de segurança mais 5.000 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

Recurso	Padrão	Comentários
Network ACLs por VPC	200	Você pode associar uma Network ACL a uma ou mais sub-redes em um VPC. Essa cota não é igual ao número de regras por Network ACL.
Regras por Network ACL	20	Esta é a cota unidirecional para uma única network ACL. Esta cota é imposta separadamente para regras de IPv4 e IPv6; por exemplo, é possível ter 20 regras de entrada para tráfego de IPv4 e 20 regras de entrada para tráfego de IPv6. Essa cota inclui as regras de negação padrão (regra número 32767 para IPv4 e 32768 para IPv6, ou um asterisco * no console da Amazon VPC). Essa cota pode ser aumentada até um número máximo de 40. No entanto, isso pode afetar o desempenho da rede devido ao aumento da carga de trabalho para processar as regras adicionais.

Interfaces de rede

Recurso	Padrão	Comentários
Interfaces de rede por instância	–	Essa cota varia de acordo com o tipo de instância. Para obter mais informações, consulte Endereços IP por ENI por tipo de instância.
Interfaces de rede por região	5000	Essa cota se aplica a VPCs individuais da conta da AWS e VPCs compartilhadas.

Tabelas de rotas

Recurso	Padrão	Comentários
Tabelas de rotas por VPC	200	A tabela de rotas principal é contabilizada de acordo com essa cota.
Rotas por tabela de rotas (rotas não propagadas)	50	Você pode aumentar essa cota até 1.000. No entanto, isso pode afetar o desempenho 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 desempenho. Se você fizer referência a uma lista de prefixos gerenciada pelo cliente em uma rota, o número máximo de entradas para as listas de prefixos será igual ao mesmo número de rotas.
Rotas BGP anunciadas por tabela de rotas (rotas propagadas)	100	Essa cota não pode ser aumentada. Se você precisar de mais de 100 prefixos, anuncie uma rota padrão.

Grupos de segurança

Recurso	Padrão	Comentários
Grupos de segurança da VPC por região	2500	Essa cota se aplica a VPCs individuais da conta da AWS e VPCs compartilhadas. Se você aumentar essa cota para mais de 5.000 grupos de segurança em uma região, recomendamos paginar as chamadas para descrever seus grupos de segurança e obter melhor desempenho.
As regras de entrada ou de saída por grupo de segurança	60	Você pode ter 60 regras de entrada e 60 regras de saída por grupo de segurança (totalizando 120 regras). Essa cota é imposta separadamente das regras IPv4 e IPv6. Por exemplo, um grupo de segurança pode ter 60 regras de entrada para tráfego IPv4 e 60 para tráfego IPv6. Uma regra que faz referência a um grupo de segurança ou ID da lista de prefixos gerenciada pela AWS conta como uma regra para IPv4 e uma regra para IPv6. Uma alteração de cota é aplicada às regras de entrada e saída. Essa cota multiplicada

Recurso	Padrão	Comentários
		pela cota para os grupos de segurança por interface de rede não pode exceder 1000. Por exemplo, se você aumentar a cota para 100, diminuiremos a cota de seu número de grupos de segurança por interface de rede para 10. Se você fizer referência a uma lista de prefixos gerenciados pelo cliente em uma regra de grupo de segurança, o número máximo de entradas para as listas de prefixos será igual ao número de regras de grupo de segurança.
Grupos de segurança por interface de rede	5	O máximo é 16. Essa cota é aplicada separadamente para as regras de IPv4 e as regras de IPv6. A cota dos grupos de segurança por interface de rede multiplicado pela cota de regras por grupo de segurança não pode exceder 1000. Por exemplo, se você aumentar essa cota para 10, diminuiremos a cota do seu número de regras por grupo de segurança para 100.

Conexões de emparelhamento de VPC

Recurso	Padrão	Comentários
Conexões emparelhadas de VPC ativas por VPC	50	A cota máxima é de 125 conexões emparelhadas por VPC. O número de entradas por tabela de rotas deve ser aumentado de acordo. No entanto, o desempenho da rede pode ser afetado.
Solicitações de conexão de emparelhamento de VPC pendentes	25	Essa é a cota do número de solicitações de conexão de emparelhamento de VPC pendentes que você solicitou da sua conta.
Hora de expiração para uma solicitação de conexão de emparelhamento de VPC não aceita	1 semana (168 horas)	Essa cota não pode ser aumentada.

VPC endpoints

Recurso	Padrão	Comentários
VPC endpoints do gateway por região	20	Você não pode ter mais de 255 endpoints de gateway por VPC.
Endpoints do Gateway Load Balancer e da interface por VPC	50	Essa é a cota combinada para o número máximo de endpoints de interface e

Recurso	Padrão	Comentários
		endpoints do Gateway Load Balancer em uma VPC. Para aumentar essa cota, entre em contato com o AWS Support.
Tamanho da política de VPC endpoints	20.480 caracteres (incluindo espaços em branco)	Essa cota não pode ser aumentada.

As seguintes regras de maximum transmission unit (MTU – unidade de transmissão máxima) aplicam-se ao tráfego que passa por um VPC endpoint.

- A MTU de uma conexão de rede é o tamanho, em bytes, do maior pacote permissível que pode ser passado pelo VPC endpoint. Quanto maior a MTU, mais dados podem ser passados em um único pacote. Um VPC endpoint é compatível com uma MTU de 8500 bytes.
- Pacotes com um tamanho maior que 8500 bytes que chegam ao VPC endpoint são descartados.
- O VPC endpoint não gera o pacote FRAG_NEEDEDICMP, portanto, o Path MTU Discovery (PMTUD) não é compatível.
- O VPC endpoint aplica o ajuste do Maximum Segment Size (MSS – Tamanho máximo de segmento) para todos os pacotes. Para obter mais informações, consulte RFC879.

Conexões do AWS Site-to-Site VPN.

Para mais informações, consulte Cotas do Site-to-Site VPN no Guia do usuário do AWS Site-to-Site VPN.

Compartilhamento da VPC

Todas as cotas padrão de VPC são aplicáveis a uma VPC compartilhada.

Recurso	Padrão	Comentários
Contas participantes por VPC	100	Essa é a cota para 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. Para aumentar essa cota, entre em contato com o AWS Support. Os proprietários da VPC podem visualizar as interfaces de rede e os grupos de segurança anexados aos recursos do participante. Portanto, a AWS recomenda paginar suas chamadas de API `DescribeSecurityGroups` e `DescribeNetworkInterfaces` antes de solicitar um aumento dessa cota.

Recurso	Padrão	Comentários
As sub-redes que podem ser compartilhadas com uma conta	100	Essa é a cota para o número máximo de sub-redes que podem ser compartilhadas com uma conta da AWS. Para aumentar essa cota, entre em contato com o AWS Support. A AWS recomenda paginar suas chamadas de API `DescribeSecurityGroups` e `DescribeSubnets` antes de solicitar um aumento dessa cota.

Controle de utilização da API do Amazon EC2

Para obter informações sobre o controle de utilização do Amazon EC2, consulte Controle de utilização de API na Referência de API do Amazon EC2.

Histórico do documento

A tabela a seguir descreve as alterações importantes em cada versão do Guia do usuário da Amazon VPC e do Guia de emparelhamento da Amazon VPC.

update-history-change	update-history-description	update-history-date
Endpoints de interface do Amazon S3	Você pode criar um endpoint de interface do Amazon S3.	2 de fevereiro de 2021
Endpoints do Gateway Load Balancer	Você pode criar um endpoint do Gateway Load Balancer na VPC para rotear o tráfego para um serviço do VPC endpoint que você configurou usando o Gateway Load Balancer.	10 de novembro de 2020
Gateways de operadora	Crie gateways de operadora para permitir o tráfego de entrada de uma rede de operadora em um local específico e o tráfego de saída para a rede de operadora e a Internet.	6 de agosto de 2020
Tag na criação (p. 352)	É possível adicionar tags ao criar uma conexão de emparelhamento de VPC e uma tabela de rotas.	20 de julho de 2020
Tag na criação (p. 352)	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
Chaves de condição para VPC endpoints e serviços de endpoint	É possível usar chaves de condição do EC2 para controlar o acesso ao VPC endpoint e aos serviços de endpoint.	6 de março de 2020

Marcação no VPC endpoint e criação de serviço do VPC endpoint.	É possível adicionar uma tag ao criar um VPC endpoint ou um serviço do VPC endpoint.	5 de fevereiro 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 console da Amazon VPC.	22 de janeiro de 2020
Nome DNS privado	Agora é possível acessar serviços baseados no AWS PrivateLink de forma privada pela VPC usando nomes DNS privados.	6 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
Emparelhamento entre regiões	A resolução do nome de host DNS é compatível com conexões de emparelhamento de VPCs entre regiões na região Ásia-Pacífico (Hong Kong).	26 de agosto de 2019
AWS Site-to-Site VPN	A VPN gerenciada pela AWS agora é conhecida como AWS Site-to-Site VPN.	18 de dezembro de 2018
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
Emparelhamento entre regiões	É possível criar uma conexão de emparelhamento de VPC entre VPCs em diferentes regiões da AWS.	29 de novembro de 2017
Serviços do VPC endpoint	É possível criar seu próprio serviço do AWS PrivateLink em uma VPC e habilitar outras contas e usuários da AWS para se conectarem ao seu serviço com um VPC endpoint de interface.	28 de novembro de 2017

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
Endpoints da VPC de interface para serviços da AWS	É possível criar um endpoint de interface para se conectar de forma privada a alguns serviços da AWS. Um endpoint de interface é uma interface de rede com um endereço IP privado que serve como ponto de entrada para tráfego ao serviço.	8 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
VPC endpoints para o DynamoDB	É possível acessar o Amazon DynamoDB a partir de sua VPC usando VPC endpoints.	16 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 (p. 352)	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
Suporte de resolução de DNS para emparelhamento de VPC	Você pode habilitar uma VPC local para que determine nomes de host DNS públicos para endereços IP privados quando em consultas provenientes de instâncias na VPC emparelhada.	28 de julho de 2016

Regras de grupo de segurança obsoletas	Você pode identificar se seu security group está sendo referido nas regras de um security group em uma VPC emparelhada e pode identificar regras de security group obsoletas.	12 de maio de 2016
Uso de ClassicLink em uma conexão de emparelhamento de VPC	Você pode modificar sua conexão de emparelhamento de VPC para permitir que instâncias locais vinculados ao EC2-Classic comuniquem-se com instâncias em uma VPC emparelhada ou vice-versa.	26 de abril 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 informações sobre o tráfego de IP para e proveniente das interfaces de rede em sua VPC.	10 de junho de 2015
VPC endpoints	Um endpoint permite que você crie uma conexão privada entre sua VPC e outro serviço da AWS sem exigir acesso pela Internet, por meio de uma conexão VPN, de uma Instância NAT ou do AWS Direct Connect.	11 de maio de 2015
ClassicLink	ClassicLink permite que você vincule sua instância do EC2-Classic a uma VPC em sua conta. Você pode associar os grupos de segurança da VPC à instância do EC2-Classic e permitir a comunicação entre sua Instância EC2-Classic e 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
Emparelhamento de VPC	É possível criar uma conexão de emparelhamento de VPC entre duas VPCs, o que permite que as instâncias em ambas as VPCs comuniquem-se entre si usando endereços IP privados.	24 de março 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 (p. 352)	Adicionado o suporte à 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 (p. 352)	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