Amazon Virtual Private Cloud

Guia de conceitos básicos

API Version 2012-12-01

Amazon Web Services

Amazon Virtual Private Cloud: Guia de conceitos básicos

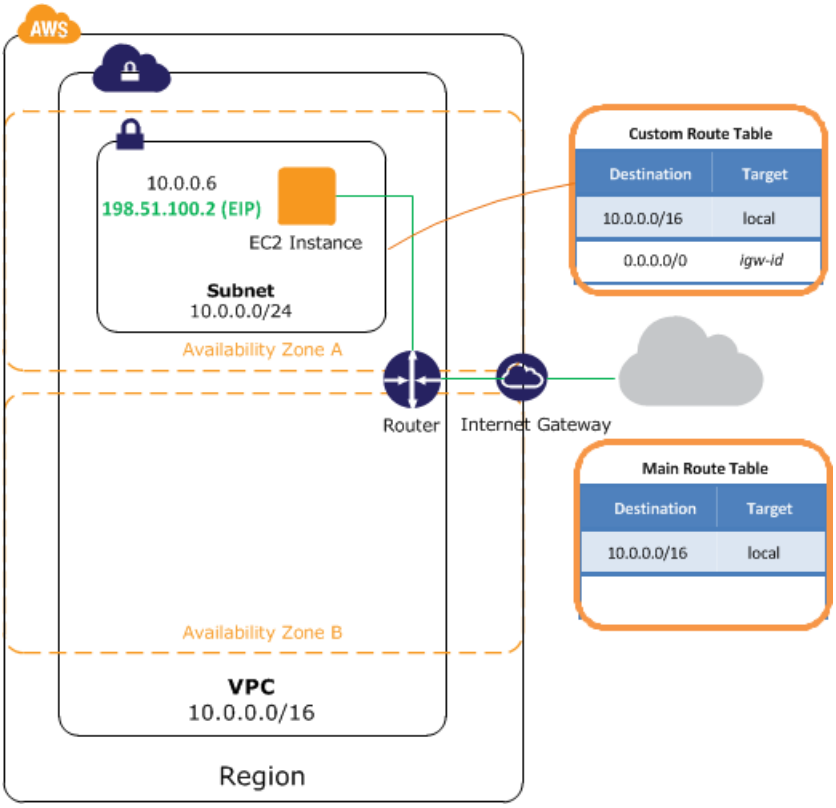
Amazon Web Services

Visão geral do exercício

Uma Virtual Private Cloud (VPC) é uma rede virtual que lembra muito uma rede tradicional que você pode operar em seu próprio Datacenter, com a vantagem de usar a infraestrutura escalável do Amazon Web Services (AWS). Após concluir as tarefas deste exercício, você terá uma instância do Amazon EC2 em execução em uma nondefault VPC que poderá ser acessada pela Internet utilizando SSH (para instâncias do Linux) ou a área de trabalho remota (para instâncias do Windows).

Para obter uma visão geral da Amazon VPC, consulte What is Amazon VPC? no *Guia do usuário da Amazon Virtual Private Cloud*.

O diagrama a seguir mostra a arquitetura que será criada após a conclusão do exercício neste guia. O grupo de segurança que você configurou e associou à instância permite apenas o tráfego por meio de portas específicas, a comunicação com a instância é bloqueada de acordo com as regras especificadas. O uso de um endereço Elastic IP (EIP) permite que uma instância em uma VPC, que normalmente seria privada, seja acessada pela Internet por meio de um gateway de Internet (por exemplo, pode atuar como um servidor da Web).



A tabela a seguir resume as tarefas que serão desempenhadas após a conclusão do exercício neste guia.

Etapa 1: cadastre-se na Amazon VPC (p. 4)	Cadastre-se na Amazon VPC caso ainda não esteja cadastrado.
Etapa 2: configurar a VPC e o gateway de Internet (p. 5)	Use o Assistente da VPC para fazer o seguinte: 1. Crie uma VPC, que é uma parte isolada da nuvem da AWS. 2. Crie e anexe um gateway de Internet, que conecta a VPC diretamente à Internet e fornece acesso a outros produtos da AWS, como o Amazon Simple Storage Service (Amazon S3). 3. Crie uma sub-rede da Amazon VPC, que é um segmento de intervalo de endereço IP da VPC que você executa dentro das instâncias do Amazon EC2. As sub-redes permitem que você agrupe instâncias com base em suas necessidades operacionais e de segurança. 4. Configure o roteamento na VPC para habilitar o tráfego entre a sub-rede e a Internet. Sua VPC tem um roteador implícito, como mostrado no diagrama.

Etapa 3: configurar um grupo de segurança para sua VPC (p. 8)	Use o console da Amazon VPC para configurar um grupo de segurança para controlar o tráfego de entrada e de saída para a instância.
Etapa 4: executar uma instância em uma VPC (p. 9)	Use o console do Amazon EC2 para executar uma instância na sub-rede. A instância tem um endereço IP privado do intervalo de endereços da sub-rede.
Etapa 5: atribua um endereço Elastic IP à instância (p. 10)	Use o console da Amazon VPC para alocar um endereço Elastic IP e atribui-lo à instância. O endereço Elastic IP oferece um endereço IP público à instância, além do endereço privado, para que a instância possa ser acessada pela Internet.
Etapa opcional: excluir a VPC (p. 10)	Use o console do Amazon EC2 para terminar sua instância e o console da Amazon VPC para excluir sua VPC.

Conceitos básicos da Amazon VPC

Este guia fornece uma introdução prática ao uso da Amazon VPC por meio do AWS Management Console. O exercício deste guia conduz você através de um cenário simples em que uma VPC é configurada com uma sub-rede pública única contendo uma instância do EC2 em execução com um endereço Elastic IP.

Topics

Para obter uma visão geral do exercício, consulte Visão geral do exercício (p. 1). Para obter uma visão geral básica da Amazon VPC, consulte What is Amazon VPC? no *Guia do usuário da Amazon Virtual Private Cloud*.

Etapa 1: cadastre-se na Amazon VPC

Quando você cria uma conta da AWS, a AWS cadastra automaticamente a conta para todos os serviços da AWS, incluindo o Amazon EC2 e a Amazon VPC. Você será cobrado apenas pelos serviços que usar. Para este exemplo, as cobranças serão mínimas.

Se você já possui uma conta da AWS, vá para a próxima etapa. Se você ainda não possui uma conta da AWS, use o procedimento a seguir para criar uma.

Para criar uma conta da AWS

1. Acesse http://aws.amazon.com e clique em Cadastrar-se.
2. Siga as instruções na tela.

   Parte do processo de cadastro envolve uma chamada de telefone e a digitação de um PIN usando o teclado do telefone.

A AWS irá notificá-lo por e-mail quando sua conta estiver ativa e disponível para uso.

Etapa 2: configurar a VPC e o gateway de Internet

Neste exercício, usaremos o assistente da VPC para criar uma VPC. O assistente realizará as seguintes etapas para você:

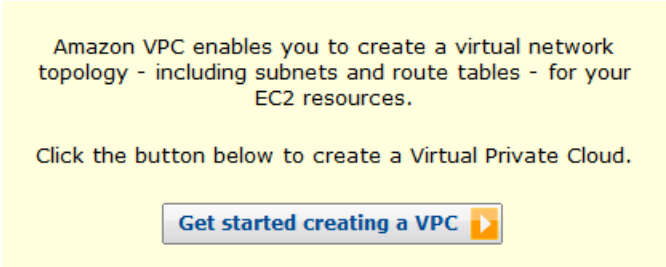
Tip

Se você preferir, poderá executar essas etapas manualmente usando o AWS Management Console.

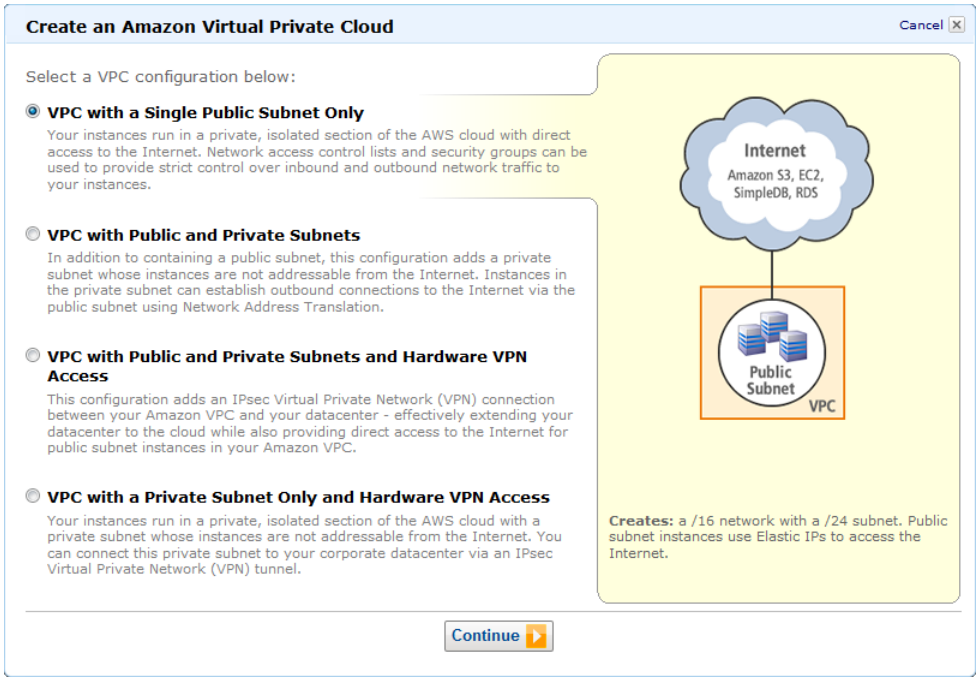
- Criar uma VPC de tamanho /16 (uma rede com 65.536 endereços IP privados).
- Anexar um gateway de Internet à VPC.
- Adicionar um subnet de tamanho /24 (um intervalo de 256 endereços IP privados).
- Configurar o roteamento na sua VPC para que o tráfego possa fluir entre o subnet e o gateway de Internet.

Para criar uma VPC usando o Assistente da VPC no AWS Management Console

1. Cadastre-se no AWS Management Console e abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel da VPC, clique em Get started creating a VPC.



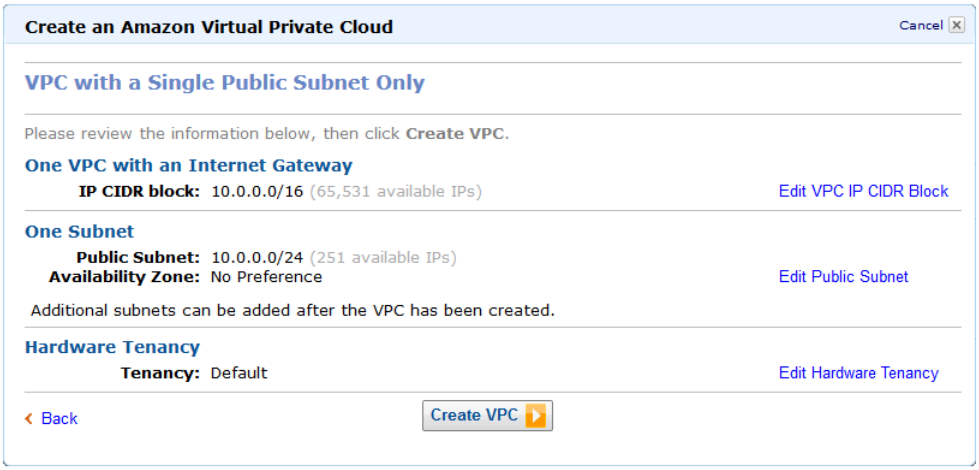
3. Para a primeira opção, selecione VPC with a Single Public Subnet Only e clique em Continue.



4. A página de confirmação mostrará os intervalos de CIDR que usaremos para sua VPC e subnet (10.0.0.0/16 e 10.0.0.0/24, respectivamente), bem como a configuração de locação de hardware. Faça quaisquer alterações nessas configurações necessárias e clique em Create VPC para criar sua VPC, gateway de Internet, sub-rede e tabela de rota.

   Note

   Para obter informações sobre notação CIDR, consulte o artigo na Wikipédia sobre roteamento sem classe entre domínios. Para obter mais informações sobre propriedade de hardware, consulte Using EC2 Dedicated Instances no *Guia do usuário da Amazon Virtual Private Cloud*.



5. Uma janela de status mostra o trabalho em andamento. Quando o trabalho for concluído, uma janela de status confirmará que sua VPC foi criada com êxito. Clique em Close para fechar a janela de status e retornar ao painel da VPC.

Verificar os componentes da VPC

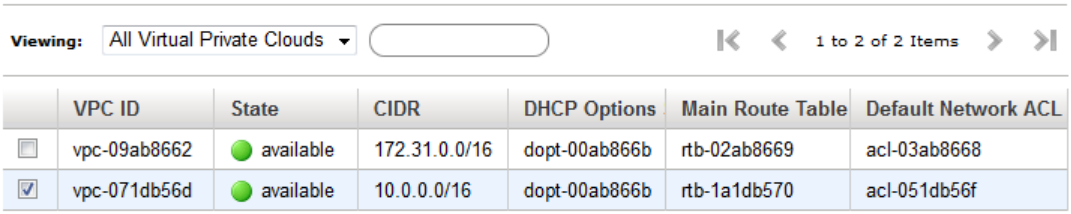
Você pode usar as configurações padrão dos componentes que o Assistente da VPC criou à medida que avança com o exercício neste guia. Esta seção descreve como você pode visualizar estes componentes e suas configurações utilizando o console da VPC.

No painel de navegação, clique em Your VPCs e, em seguida, selecione a VPC recém-criada.

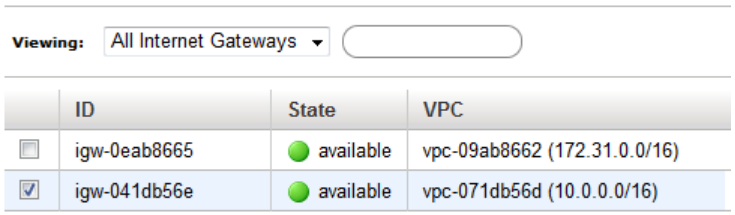
Tip

Talvez você precise atualizar a página para que a VPC apareça.

O console exibe a VPC recém-criada. Todas as VPCs têm um conjunto de opções DHCP, uma tabela de rota principal e ACLs de rede padrão. Para obter mais informações, vá para DHCP Options Sets, Route Tables e Network ACLs no *Guia do usuário da Amazon Virtual Private Cloud*.



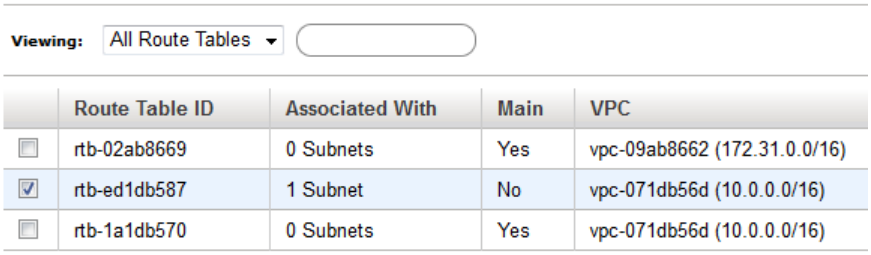
Para exibir informações sobre seus gateways de Internet, clique em Internet Gateways no painel de navegação.



A VPC recém-criada tem duas tabelas de rota. A VPC vem com uma tabela de rota principal padrão e, além dela, o Assistente da VPC criou uma tabela de rota personalizada. Sua sub-rede é associada com a tabela de rota personalizada, o que significa que usamos as rotas nessa tabela para determinar como o tráfego da sub-rede flui. Se você adicionar uma nova sub-rede à VPC, a tabela de rota principal será usada como padrão.

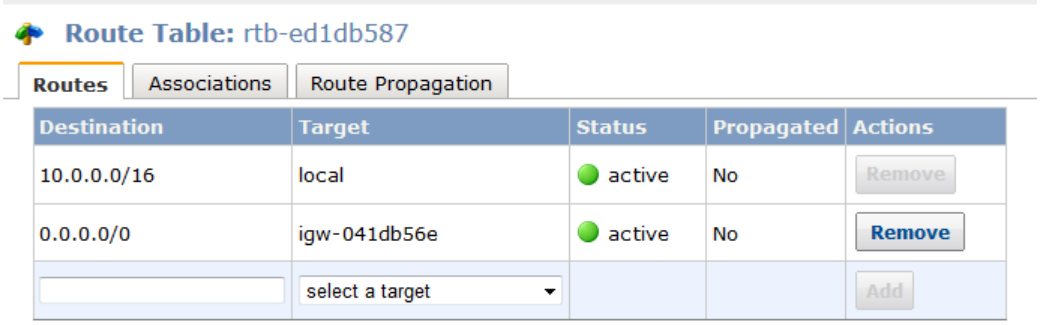
Para visualizar as tabelas de rota

1. Clique em Route Tables no painel de navegação.
2. Selecione a tabela de rota personalizada (a coluna Main tem No) para exibir as informações no painel de detalhes.

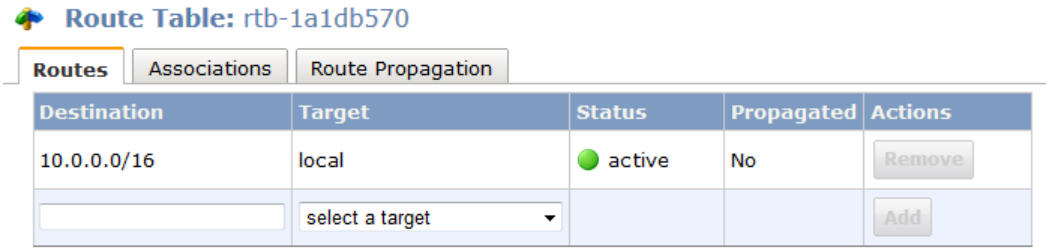


3. A primeira linha na tabela é a rota local, que permite instâncias na VPC para comunicar. Essa rota está presente em toda tabela de rota por definição e não pode ser removida.

   A segunda linha mostra a rota que o assistente da VPC adicionou para permitir que o tráfego destinado para qualquer endereço IP fora da VPC (0.0.0.0/0) flua da sub-rede para o gateway de Internet. Essa sub-rede é denominada *pública* porque todo o tráfego da sub-rede vai para o gateway de Internet.



4. Selecione a tabela de rota principal. A tabela de rota principal tem uma rota local, mas não há outras rotas. Portanto, qualquer sub-rede nova que você cria inicialmente não está exposta à Internet (ou seja, é *privada*). Se você decidir expor uma nova sub-rede como uma sub-rede pública, poderá alterar o roteamento na tabela de rota principal ou associar a sub-rede a uma tabela de rota personalizada.



Etapa 3: configurar um grupo de segurança para sua VPC

Um *grupo de segurança* atua como um firewall virtual para controlar o tráfego permitido para as instâncias associadas. Para usar grupos de segurança, crie um grupo, adicione as regras de entrada e saída que deseja usar e associe suas instâncias ao grupo de segurança quando executá-las. Se você adicionar

ou remover regras do grupo de segurança, aplicaremos estas alterações à instância associada ao grupo de segurança automaticamente.

Sua VPC é fornecida com um *grupo de segurança padrão*. As instâncias não associadas a outro grupo de segurança serão associadas ao grupo de segurança padrão. Embora fosse possível usar o grupo de segurança padrão para este exercício, preferimos criar um grupo de segurança`WebServerSG`. Especifique este grupo de segurança quando você executar uma instância na VPC.

Topics

Regras para o grupo de segurança WebserverSG

As regras de entrada regulam o tráfego permitido para acesso às instâncias associadas ao grupo de segurança (a origem do tráfego e a porta de escuta na instância). Todo o tráfego de retorno é automaticamente autorizado a acessar as instâncias. Por exemplo, se um cliente na Internet envia uma solicitação para um servidor da Web em sua VPC associada à `WebServerSG`, a instância pode responder, independentemente de quaisquer regras de saída do grupo. Desta forma, grupos de segurança têm monitoração de estado.

As regras de saída controlam para quais destinos as instâncias associadas ao grupo de segurança podem enviar tráfego (o destino do tráfego e a porta de destino). Todo o tráfego de retorno (como uma resposta do host que recebeu o tráfego) recebe automaticamente permissão de acesso às instâncias, independentemente das regras de entrada definidas no grupo de segurança.

A tabela a seguir relaciona as regras de entrada e saída para o grupo de segurança `WebServerSG` e o que elas fazem.

Note

Se sua empresa utiliza somente Linux ou somente Windows, você não precisa adicionar acesso para SSH e RDP.

Entrada			
IP de origem	Protocol	Intervalo de Portas	Comentários
0.0.0.0/0	TCP	80	Permitir acesso HTTP de entrada de qualquer lugar
0.0.0.0/0	TCP	443	Permitir acesso HTTPS de entrada de qualquer lugar
Intervalo de endereços IP públicos da sua rede doméstica	TCP	22	Permitir acesso SSH de entrada de sua rede doméstica (somente Linux/UNIX)
Intervalo de endereços IP públicos da sua rede doméstica	TCP	3389	Permitir acesso RDP de entrada de sua rede doméstica (somente Windows)

Saída			
Dest IP	Protocol	Intervalo de Portas	Comentários
0.0.0.0/0	TCP	80	Permitir o acesso de saída HTTP para servidores na Internet (por exemplo, atualizações de software)
0.0.0.0/0	TCP	443	Permitir o acesso de saída HTTPS para servidores na Internet (por exemplo, atualizações de software)

Neste exercício, você não adicionará uma regra para permitir a comunicação entre instâncias associadas ao grupo de segurança. Para permitir esse tipo de comunicação, é preciso adicionar uma regra ao grupo de segurança para este propósito. Para obter mais informações, consulte Security Groups em *Guia do usuário da Amazon Virtual Private Cloud*.

Como criar o seu grupo de segurança WebserverSG

Para criar o grupo de segurança WebServerSG

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. Clique em Security Groups no painel de navegação.
3. Clique no botão Create Security Group.
4. Insira `WebServerSG` como o nome do grupo de segurança e forneça uma descrição. Selecione o ID de sua VPC no menu VPC e clique em Yes, Create.

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.

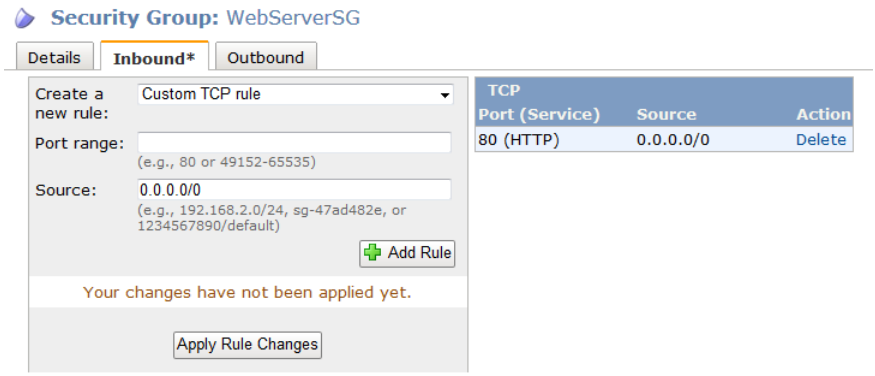
Como adicionar regras ao grupo de segurança WebserverSG

Para adicionar regras ao grupo de segurança WebserverSG

1. Clique em Security Groups no painel de navegação para exibir seus grupos de segurança.
2. Selecione o grupo de segurança `WebServerSG` que você acabou de criar. O painel de detalhes inclui uma guia de informações sobre o grupo de segurança, além de guias para trabalhar com as regras de entrada e de saída do grupo.
3. Adicionar regras de acesso HTTP e HTTPS de entrada de qualquer lugar:

    a. Na guia Inbound, selecione `HTTP` na lista suspensa Create a new rule e certifique-se de que a opção Source seja `0.0.0.0/0`.

    b. Clique em Add Rule. Isso adiciona uma regra para permitir acesso HTTP de qualquer lugar. Observe que o botão Apply Rule Changes está ativado e o texto "Your changes have not been applied yet" aparece acima do botão. Clicaremos neste botão para aplicar as alterações à regra depois que adicionarmos todas as regras de entrada.



c. Selecione `HTTPS` na lista suspensa Create a new rule e certifique-se de que a opção Source seja `0.0.0.0/0`.

d. Clique em Add Rule. Isso adiciona uma regra para permitir acesso HTTPS de qualquer lugar.

4. Adicionar regras de acesso SSH de entrada e de área de trabalho remota (RDP) para o grupo do intervalo de endereços IP públicos da rede:

Caution

Ao usar o `0.0.0.0/0`, você permite que todos os endereços IP acessem sua instância usando o SSH ou o RDP. Isso é aceitável para um exercício rápido, mas não é seguro para ambientes de produção. Em produção, você vai autorizar apenas um endereço IP específico ou intervalo de endereços para acessar a instância.

Tip

Você também pode obter um endereço IP público de seu computador local que utiliza um serviço. Para localizar um serviço que fornece seu endereço IP, use a frase de busca "what is my IP address". Se você estiver conectado por meio de um ISP ou atrás de um firewall sem um endereço IP estático, terá de localizar o intervalo de endereços IP usado por computadores cliente.

a. Na guia Inbound, selecione`SSH` na lista suspensa Create a new rule.

b. No campo Source, insira o seu intervalo de endereços IP públicos da rede (por exemplo, 192.0.2.0/24). Se você não souber o intervalo de endereços, poderá usar `0.0.0.0/0` para este exercício (consulte a "Caution and Tip" desta etapa).

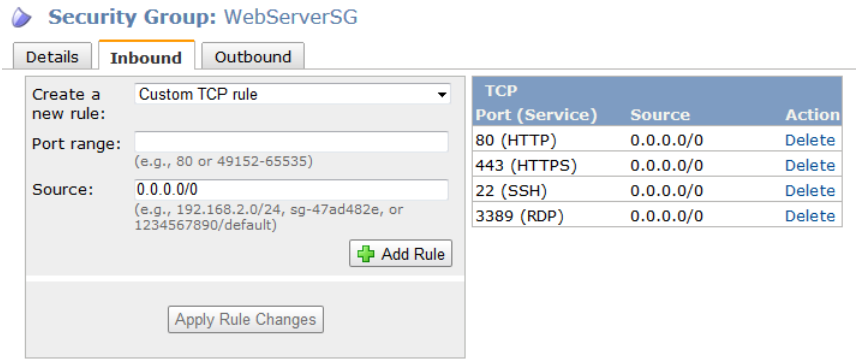
c. Clique em Add Rule.

d. Selecione `RDP` na lista suspensa Create a new rule.

e. No campo Source, insira o intervalo de endereços IP públicos da rede doméstica. Se você não souber qual é este intervalo de endereços, poderá usar `0.0.0.0/0` para este exercício (consulte a "Caution and Tip" desta etapa).

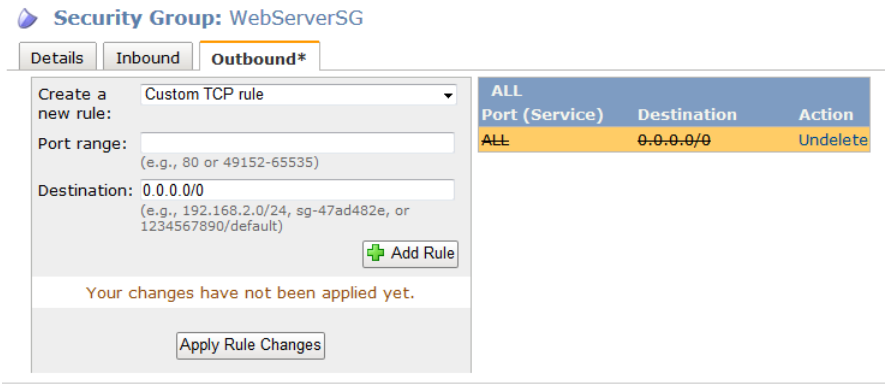
f. Clique em Add Rule.

5. Clique em Apply Rule Changes para aplicar essas regras de entrada.



6. Limitar o acesso de saída para apenas HTTP e HTTPS do grupo para qualquer lugar:

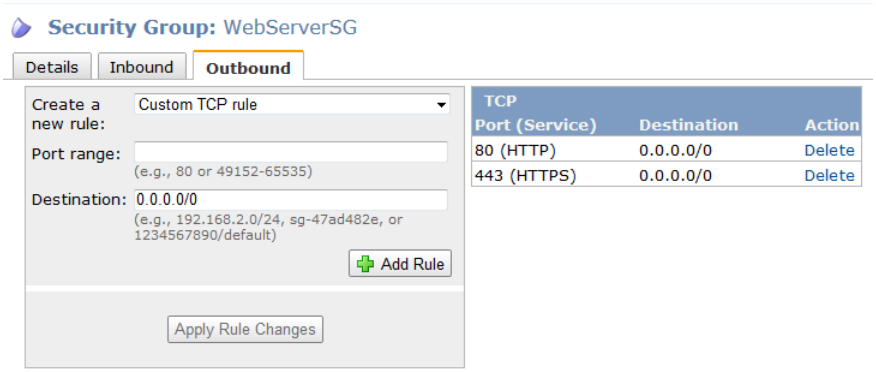
   a. Na guia Outbound, localize a regra padrão que permite todo o tráfego de saída e clique em Delete. A regra é marcada para exclusão. No entanto, esta alteração não será aplicada até que você clique em Apply Rule Changes. Isso só será feito depois que você adicionar as regras de saída para HTTP e HTTPS.



   b. SelecioneHTTP na lista suspensa Create a new rule e clique em Add Rule. Isso adiciona uma regra para permitir acesso de saída HTTP de qualquer lugar.

   c. SelecioneHTTPS na lista suspensa Create a new rule e clique em Add Rule. Isso adiciona uma regra para permitir acesso de saída HTTPS de qualquer lugar.

7. Clique em Apply Rule Changes para aplicar essas regras de saída.

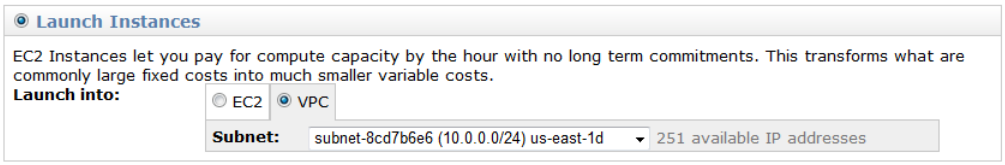


Etapa 4: executar uma instância em uma VPC

Quando você executa uma instância do EC2 em uma VPC, é preciso especificar o ID da sub-rede na VPC.

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, selecione a região da instância. Para este exercício, você pode usar a região padrão. Para obter mais informações sobre regiões e zonas de disponibilidade, consulte Regions and Availability Zones no *Guia do usuário do Amazon Elastic Compute Cloud*.
3. No painel, clique no botão Launch Instance.
4. Na página Create a New Instance, selecione Classic Wizard. Em seguida, clique em Continue.
5. Na página CHOOSE AN AMI, a guia Quick Start exibirá uma lista de configurações básicas denominadas Imagens de máquina da Amazon (AMI). Escolha a AMI que deseja usar e clique no seu botão Select.
6. Na página INSTANCE DETAILS, no menu Instance Type, mantenha o valor padrão, Micro (t1.micro), para executar uma microinstância individual.
7. Em Launch Instances, confirme se sua sub-rede está selecionada na caixa de listagem suspensa Subnet e clique em Continue.



8. Em Advanced Instance Options, você pode especificar o endereço IP a ser usado para a instância. No entanto, para este exercício, deixe o IP Address em branco e clique em Continue para aceitar as configurações padrão.
9. Clique em Continue para usar o dispositivo de armazenamento padrão.
10. Especifique todas as tags necessárias para sua instância e clique em Continue.
11. Na página Create Key Pair, você pode selecionar um par de chaves existente ou criar um novo. Para este exercício, criaremos um par de chaves.

    a. Clique em Create a new Key Pair.
    b. Insira um nome para o seu par de chaves (por exemplo, `VPC_Keypair`) e clique em Create & Download your Key Pair. Você precisará do conteúdo da chave privada para conectar-se à sua instância depois que ela for executada. O Amazon Web Services não mantém a parte privada dos pares de chaves.
    c. Quando solicitado, salve a chave privada em um lugar seguro no sistema e clique em Continue.

12. Na página CONFIGURE FIREWALL, selecione Choose one or more of your existing Security Groups. Selecione o `WebServerSG` grupo que criou anteriormente e clique em Continue.
13. Na página REVIEW, verifique suas configurações. Quando estiver satisfeito com suas seleções, clique em Launch para executar sua instância.

Etapa 5: atribua um endereço Elastic IP à instância

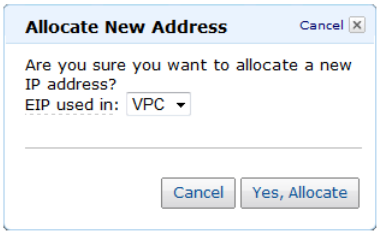
Por definição, uma instância em uma VPC é privada. Você pode tornar pública uma instância em uma VPC ao anexar um gateway de Internet à VPC e ao fornecer à instância um endereço IP público. Neste exercício, o assistente da VPC foi usado para criar um gateway de Internet para a VPC. Agora, crie um endereço Elastic IP address, que é um endereço IP público que pertence à sua conta da AWS, e associe-o à instância para ser acessado pela Internet.

Para obter informações sobre endereços Elastic IP, consulte Elastic IP Addresses no *Guia do usuário da Amazon Virtual Private Cloud*.

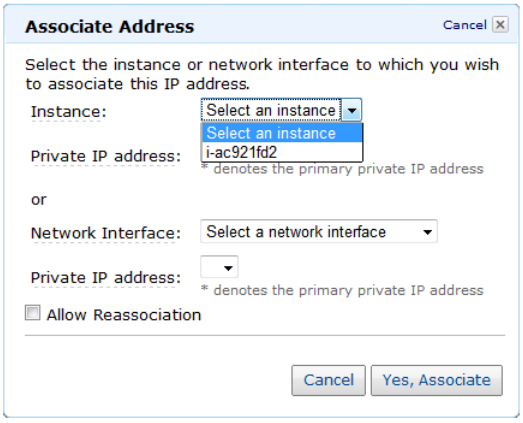
Para alocar e atribuir um endereço Elastic IP

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. Clique em Elastic IPs no painel de navegação.
3. Clique no botão Allocate New Address.

4. Na lista EIP used in:, selecione VPC e clique em Yes, Allocate.



5. Selecione o novo endereço Elastic IP na lista e clique no botão Associate Address.
6. Na caixa de diálogo Associate Address, selecione a instância a ser associada ao endereço e clique em Yes, Associate.



A instância agora pode ser acessada pela Internet. Você também pode acessar a instância usando SSH ou área de trabalho remota de sua rede doméstica, especificando o endereço Elastic IP da instância como o endereço para se conectar. Para obter instruções sobre como se conectar a uma instância do Linux, consulte Connect to Your Linux Instance no *Guia do usuário do Amazon Elastic Compute Cloud*.

Para obter instruções sobre como se conectar a uma instância do Windows, consulte Connect to Your Linux Instance no *Amazon Elastic Compute Cloud Microsoft Windows Guide*.

Isso conclui o exercício. Você tem sua VPC configurada, uma instância em execução na VPC e a capacidade de se conectar à sua instância pela Internet. Você pode continuar a usar sua instância e sua VPC ou pode finalizar a instância e excluir a VPC. Para obter informações sobre a exclusão da VPC ou sobre como localizar a documentação adicional da VPC, consulte Para onde ir agora? (p. 16).

Para onde ir agora?

Topics

Se você concluiu o exemplo neste guia, configurou uma VPC e executou uma instância nessa VPC. Você pode continuar a usar sua VPC, se desejar. Ou pode excluí-la. Excluindo-a ou não, também é possível criar outras VPCs.

Etapa opcional: excluir a VPC

Antes de excluir a VPC, é preciso finalizar as instâncias em execução na VPC. Ao excluir uma VPC, os recursos associados a ela também são excluídos, como sub-redes, grupos de segurança, ACLs de rede, conjuntos de opções DHCP, tabelas de rota e gateways de Internet.

Para excluir sua VPC

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Clique em Instances no painel de navegação.
3. Clique com o botão direito na instância em execução na VPC e selecione Terminate.
4. Quando a confirmação for solicitada, clique em Yes, Terminate.
5. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
6. Clique em Your VPCs no painel de navegação.
7. Selecione a VPC e clique no botão Delete.
8. Quando a confirmação for solicitada, clique em Yes, Delete.

Conta da AWS e credenciais de segurança

Este guia forneceu as etapas para que você pudesse se cadastrar no serviço, obter uma conta da AWS e concluir um exercício rápido. Agora que você concluiu o exercício, recomendamos que você verifique com o administrador ou com um colega de trabalho na sua empresa para determinar se eles já têm uma conta da AWS e credenciais de segurança para uso em futuras interações com a AWS.

Se você é um proprietário de conta ou administrador e gostaria de saber mais sobre o AWS Identity and Access Management, acesse http://aws.amazon.com/iam e Using AWS Identity and Access Management.

Segurança adicional para sua VPC

Se desejar outra camada de segurança além do grupo de segurança, você poderá utilizar uma lista de controle de acesso à rede (ACL). ACLs de rede controlam o tráfego no nível de subnet. Este exercício usa apenas grupos de segurança que controlam o tráfego no nível da instância. Para saber mais sobre ACLs de rede, consulte Network ACLs no *Guia do usuário da Amazon Virtual Private Cloud*.

Outros cenários para a Amazon VPC

Este guia apresenta um cenário simples do Amazon VPC. O assistente da VPC oferece outros cenários. Para obter argumentações detalhadas destes cenários, acesse Scenarios for Amazon VPC no *Guia do usuário da Amazon Virtual Private Cloud*.

Formas de acessar a Amazon VPC

Este guia mostrou como usar o Amazon VPC por meio do AWS Management Console. Você pode continuar usando o serviço por meio do console, ou você pode tentar uma das outras interfaces.

Continuar a usar o console

Para saber mais sobre como usar a Amazon VPC por meio do console, acesse Guia do usuário da Amazon Virtual Private Cloud.

Usar a interface de linha de comando

O Amazon EC2 e a Amazon VPC compartilham uma interface de linha de comando baseada em Java. Essas ferramentas de linha de comando são uma maneira rápida de usar o Amazon EC2 sem a necessidade de codificar para a API ou usar uma biblioteca. Para obter informações sobre como começar a utilizar as ferramentas de linha de comando, consulte Getting Started with the Command Line Tools no *Guia do usuário do Amazon Elastic Compute Cloud*. Para obter uma descrição completa dos comandos, consulte Amazon Elastic Compute Cloud Command Line Reference.

Usar uma biblioteca existente

O Amazon EC2 e a Amazon VPC compartilham a mesma interface programática. Se você preferir usar a Amazon VPC por meio de uma API, haverá bibliotecas e recursos disponíveis para as seguintes linguagens:

- Java

- PHP
- Python
- Ruby
- Windows e .NET

Para obter bibliotecas e exemplos de código em todas as linguagens, acesse Código & bibliotecas de exemplo do Amazon EC2.

Codificar diretamente para a API de serviços da web

Se você quiser escrever o código diretamente para a API do Amazon EC2 e da Amazon VPC, consulte Making API Requests no *Guia do usuário do Amazon Elastic Compute Cloud*. O guia descreve como criar e autenticar solicitações de API, e como usar o Amazon EC2 e a Amazon VPC por meio de APIs. Para obter uma descrição completa das ações da API, consulte Amazon Elastic Compute Cloud API Reference.

Documentação de apoio

Este Guia de Conceitos Básicos da Amazon VPC aborda as noções básicas do uso da Amazon VPC. A tabela a seguir lista outras documentações da Amazon VPC.

Descrição	Documentação
Informações sobre como usar a Amazon VPC	Guia do usuário da Amazon Virtual Private Cloud
Informações sobre como configurar o gateway cliente (se você decidir usar uma conexão VPN com a VPC)	Amazon Virtual Private Cloud Network Administrator Guide
Uma introdução prática ao Amazon EC2	Introdução ao Amazon EC2
Informações sobre como usar o Amazon EC2	Guia do usuário do Amazon Elastic Compute Cloud
Descrições dos comandos do Amazon EC2 e da Amazon VPC	Amazon Elastic Compute Cloud Command Line Reference
Descrições da API de ações, tipos de dados e erros do Amazon EC2 e da Amazon VPC.	Amazon Elastic Compute Cloud API Reference
Descrições de referência rápida de comandos frequentemente usados da Amazon VPC	Amazon Virtual Private Cloud Quick Reference Card

Onde obter mais ajuda

Recomendamos que você aproveite os fóruns de discussão da AWS. São fóruns baseados na comunidade de usuários que discutem questões técnicas relacionadas aos serviços AWS. Para o fórum da Amazon VPC, acesse https://forums.aws.amazon.com/forum.jspa?forumID=58.

Você também pode obter ajuda assinando o AWS Premium Support, um canal de suporte individual com respostas rápidas. Para obter mais informações, acesse http://aws.amazon.com/premiumsupport.

Forneça seu feedback

Sua opinião é importante para ajudar a tornar nossa documentação útil e fácil de usar. Conte-nos sobre sua experiência inicial com o uso da Amazon VPC preenchendo nossa Pesquisa sobre a primeira utilização.

Obrigado.