# **Aula 5 - criar uma nuvem privada virtual**

## **Visão geral e objetivos do laboratório**

A rede tradicional é difícil. Envolve equipamentos, cabeamento, configurações complexas e habilidades especializadas. O Amazon Virtual Private Cloud (Amazon VPC) oculta a complexidade e simplifica a implantação de redes privadas seguras.

Este laboratório mostra como criar sua própria nuvem privada virtual (VPC), implantar recursos e criar conexões de peering privado entre VPCs.

Depois de concluir este laboratório, você deverá ser capaz de:

* Implantar uma VPC
* Criar e associar um gateway de Internet à VPC
* Criar uma sub-rede pública
* Criar sub-rede privada
* Criar um servidor de aplicações para testar a VPC

## **Duração**

Este laboratório levará aproximadamente **30 minutos** para ser concluído.

## **Restrições de serviço da AWS**

Neste ambiente de laboratório, o acesso aos serviços e às ações de serviços da AWS pode ser restrito aos necessários para concluir as instruções do laboratório. Você poderá encontrar erros se tentar acessar outros serviços ou executar ações além das descritas neste laboratório.

Ao **final** deste laboratório, a arquitetura será parecida com o seguinte exemplo:



## **Acessar o console de gerenciamento da AWS**

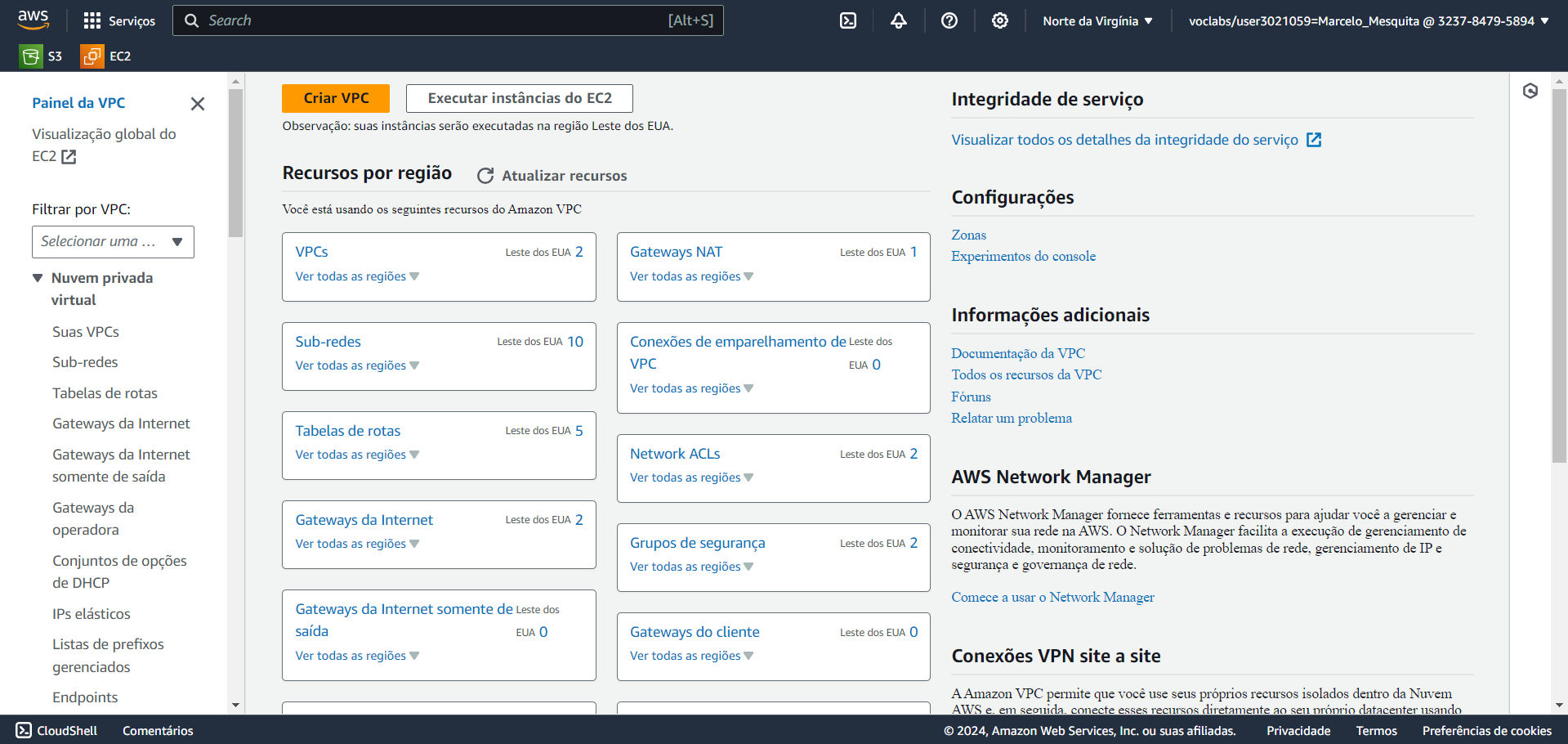
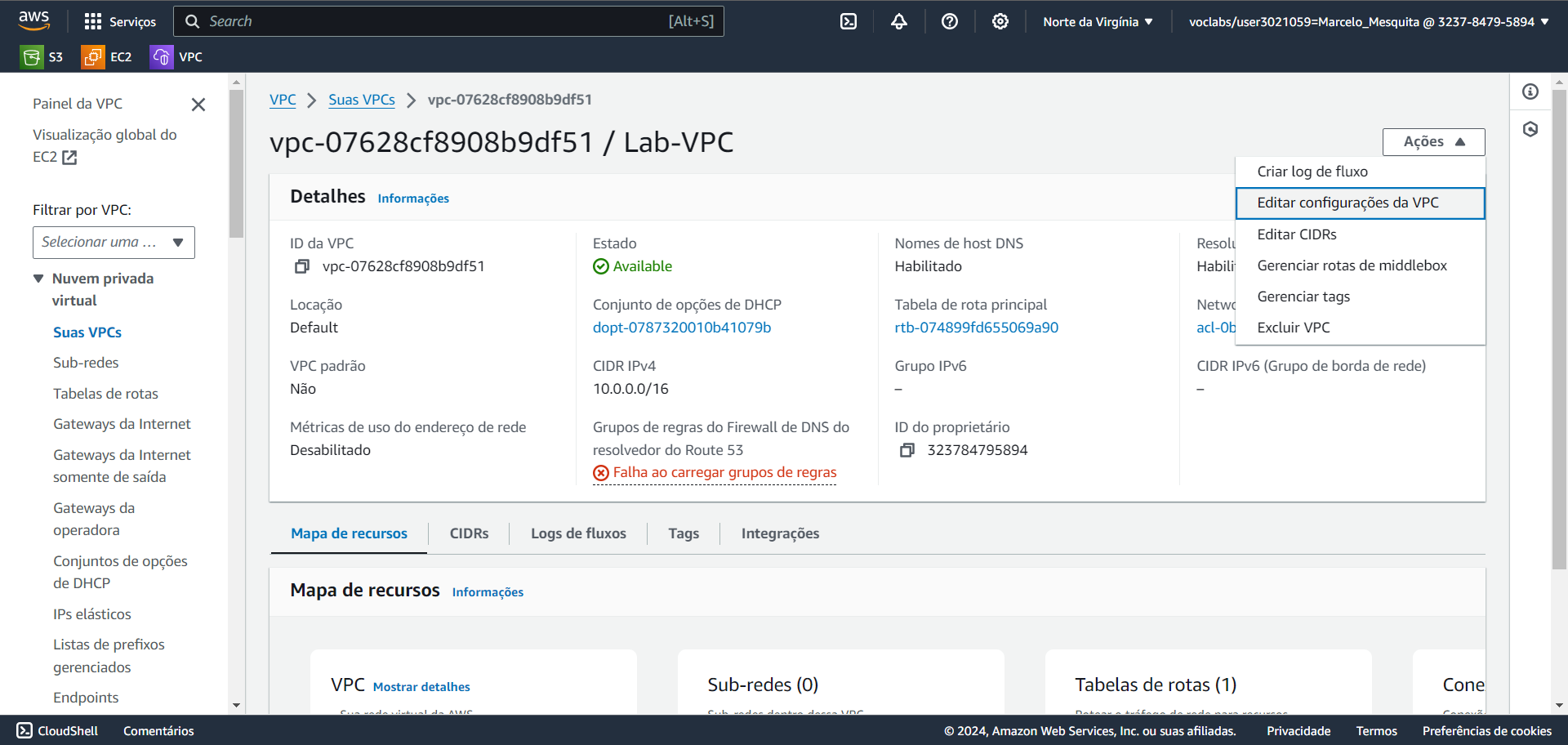
1. Na parte superior destas instruções, clique em Iniciar laboratório para iniciar o laboratório.  
   Um painel **Iniciar laboratório** é aberto com o status do laboratório.  
    **Dica**: se você precisar de mais tempo para concluir o laboratório, selecione o botão Iniciar laboratório novamente para reiniciar o cronômetro do ambiente.
2. Aguarde até que o painel **Iniciar laboratório** exiba a mensagem *Lab status: ready* (Status do laboratório: pronto) e, depois, clique no **X** para fechar o painel.
3. Na parte superior destas instruções, selecione AWS.  
   Essa ação abrirá o Console de Gerenciamento da AWS em uma nova guia do navegador. O sistema faz seu login automaticamente.  
    **Dica**: se uma nova guia não for aberta, você verá um banner ou um ícone na parte superior do navegador com uma mensagem informando que o navegador está impedindo que o site abra janelas pop-up. Clique no banner ou no ícone e selecione **Allow pop-ups** (Permitir pop-ups).
4. Organize a guia do **console de gerenciamento da AWS** para que ela seja exibida com essas instruções. De preferência, deixe as duas guias do navegador abertas ao mesmo tempo para facilitar o acompanhamento das etapas do laboratório.  
    **Não altere a região, a menos que seja especificamente instruído a fazer isso**.

## 

## **Tarefa 1: criar uma VPC**

Você começará usando o Amazon VPC para criar uma nova **nuvem privada virtual, ou VPC**.

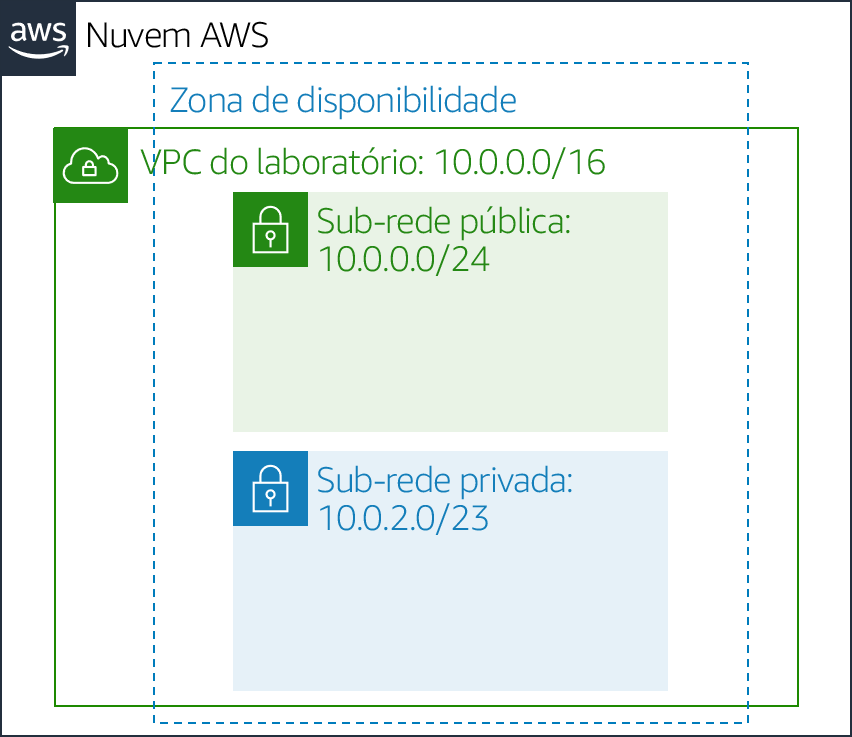
Uma VPC é uma rede virtual dedicada à sua conta do Amazon Web Services (AWS). Ela oferece isolamento lógico das outras redes virtuais na nuvem AWS. Você pode executar recursos da AWS, como instâncias do Amazon Elastic Compute Cloud (Amazon EC2), na VPC. Você pode configurar a VPC modificando seu intervalo de endereços IP e pode criar sub-redes. Você também pode configurar tabelas de rotas, gateways de rede e configurações de segurança.

1. Na caixa de pesquisa à direita de **Serviços**, procure e selecione **VPC** para abrir o console da VPC.  
   O console da VPC oferece um assistente que pode criar automaticamente várias arquiteturas de VPC. No entanto, neste laboratório, você criará os componentes da VPC manualmente.
2. No painel de navegação à esquerda, selecione **Suas VPCs**.  
   Uma VPC padrão é fornecida para que você possa executar recursos assim que começar a usar a AWS. Há também uma **VPC compartilhada**, que você usará mais tarde no laboratório. No entanto, você criará agora seu próprio *Lab VPC*.  
   A VPC terá um intervalo de Roteamento sem classe entre domínios (CIDR) de **10.0.0.0/16**, que inclui todos os endereços IP que começam com **10.0.x.x**. Ele contém mais de 65 mil endereços. Posteriormente, você dividirá os endereços em *sub-redes* separadas.
3. Selecione **Criar VPC** e defina estas configurações:
   * **Tag de nome:** **Lab VPC**
   * **IPv4 CIDR block** (Bloco CIDR IPv4): **10.0.0.0/16**
   * Selecione **Criar VPC**.  
     Uma mensagem indicando que a VPC foi criada com êxito é exibida.
4. Na metade inferior da página, selecione a guia **Tags**.  
   Tags são úteis para identificar recursos. Por exemplo, você pode usar uma tag para identificar centros de custo ou ambientes diferentes (como desenvolvimento, teste ou produção).
5. Selecione **Ações** e **Editar configurações da VPC**.  
   Essa opção atribui um nome de sistema de nomes de domínio (DNS) *amigável* às instâncias do EC2 na VPC, como:  
   ***ec2-52-42-133-255.us-west-2.compute.amazonaws.com*** **
6. Selecione **Enable DNS hostname** (Ativar nome de host DNS) e clique em **Salvar**.  
    Todas as instâncias do EC2 executadas na VPC agora receberão automaticamente um nome de host DNS. Você também pode adicionar um nome DNS mais significativo (por exemplo, *app.example.com*) posteriormente usando o Amazon Route 53.

## **Tarefa 2: criar sub-redes**

Uma sub-rede é um subintervalo de endereços IP na VPC. Os recursos da AWS podem ser executados em uma sub-rede especificada. Use uma *sub-rede pública* para recursos que devem estar conectados à Internet e use uma *sub-rede privada* para recursos que devem permanecer isolados da Internet.

Nesta tarefa, você criará uma sub-rede pública e uma sub-rede privada:



### **Criar uma sub-rede pública**

A sub-rede pública será usada para recursos voltados para a internet.

1. No painel de navegação à esquerda, selecione **Sub-redes**.
2. Selecione **Criar sub-rede** e defina estas configurações:
   * **ID da VPC:** **Lab VPC**
   * **Nome da sub-rede:** **Public Subnet**
   * **Zona de disponibilidade:** selecione a *primeira* zona de disponibilidade na lista (*não* mantenha o padrão Sem preferência)
   * **IPv4 CIDR block** (Bloco CIDR IPv4): **10.0.0.0/24**
   * Selecione **Criar sub-rede** A VPC tem um bloco CIDR de *10.0.0.0/16*, que inclui todos os endereços IP *10.0.x.x*. A sub-rede que você acabou de criar tem um bloco CIDR de *10.0.0.0/24*, que inclui todos os endereços IP *10.0.0.x*. Eles podem parecer semelhantes, mas a sub-rede é menor que a VPC devido ao */24* no intervalo de CIDR.  
     Agora, você vai configurar a sub-rede para atribuir um endereço IP público automaticamente a todas as instâncias iniciadas nela.
3. Selecione **Ações** e **Editar configurações de sub-rede** e, depois:
   * Selecione **Enable auto-assign public IPv4 address** (Habilitar endereço IPv4 Público de atribuição automática).
   * Clique em **Salvar** Mesmo que essa sub-rede tenha o nome de *Public Subnet* (Sub-rede pública), ela ainda não é pública. Uma sub-rede pública deve ter um gateway de Internet, que você irá anexar na próxima tarefa.

### 

### **Criar uma sub-rede privada**

A sub-rede privada será usada para recursos que devem permanecer isolados da internet.

1. Use o que você acabou de aprender para criar outra sub-rede com estas configurações:
   * **ID da VPC:** **Lab VPC**
   * **Nome da sub-rede:** **Private Subnet**
   * **Zona de disponibilidade:** selecione a *primeira* zona de disponibilidade na lista (*não* mantenha o padrão Sem preferência)
   * **IPv4 CIDR block** (Bloco CIDR IPv4): **10.0.2.0/24**  
     O bloco CIDR *10.0.2.0/23* inclui todos os endereços IP que começam com *10.0.2.x* e *10.0.3.x*. Isso é duas vezes maior que a sub-rede pública porque a maioria dos recursos deve ser mantida privada, a menos que devam especificamente estar acessíveis pela Internet.  
     Sua VPC agora tem duas sub-redes. No entanto, a sub-rede pública é totalmente isolada e não pode se comunicar com recursos fora da VPC. Em seguida, você vai configurar a sub-rede pública para se conectar à Internet por um gateway de Internet.

## 

## **Tarefa 3: criar um gateway de Internet**

Um *gateway de Internet* é um componente da VPC dimensionado horizontalmente, redundante e altamente disponível. Ele permite a comunicação entre instâncias na VPC e na Internet. Ele não impõe nenhum risco de disponibilidade ou restrições de largura de banda no tráfego da rede.

Um gateway de Internet tem duas finalidades:

* Fornecer um destino para que as tabelas de rotas se conectem à Internet
* Executar a conversão de endereços de rede (NAT) para instâncias que receberam endereços IPv4 públicos

Nesta tarefa, você criará um gateway de internet para que o tráfego da internet possa acessar a sub-rede pública.

1. No painel de navegação à esquerda, selecione **Gateways da Internet**.
2. Selecione **Criar gateway da Internet** e defina estas configurações:
   * **Tag de nome:** **Lab IGW**
   * Selecione **Criar gateway da Internet**.
3. Agora, você pode anexar o gateway de Internet ao *Lab VPC*. Selecione **Ações** e **Anexar à VPC** e defina estas configurações:
   * **VPCs disponíveis:** coloque o cursor na caixa de pesquisa e selecione *Lab VPC*
   * Selecione **Associar gateway da Internet**.( Associar à VPC )  
     Esta ação associará o gateway de Internet ao seu *Lab VPC*. Mesmo que você tenha criado um gateway de Internet e associado à sua VPC, também deve configurar a *tabela de rotas* da sub-rede pública para usar o gateway de Internet.

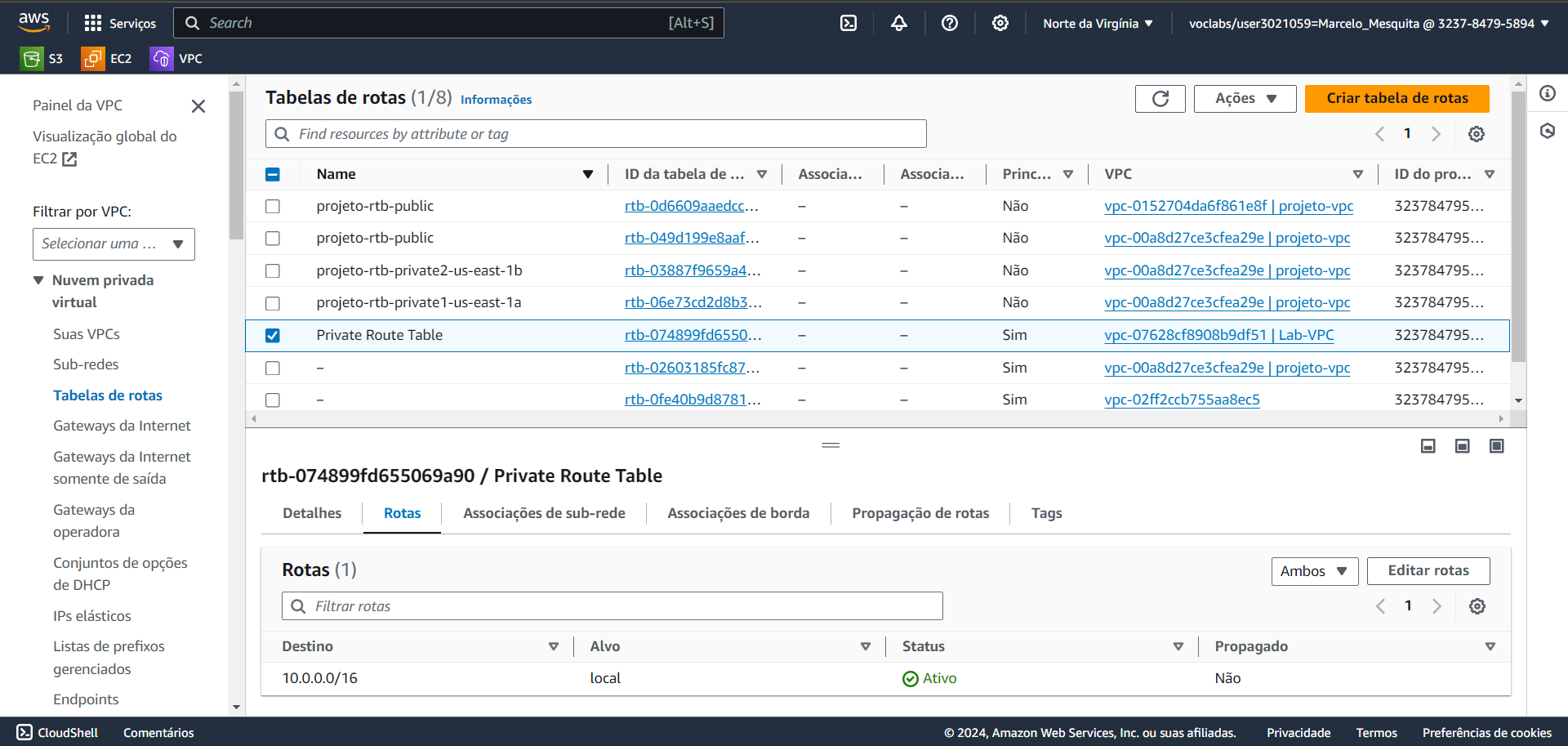
## **Tarefa 4: configurar tabelas de rotas**

A *tabela de rota* contém um conjunto de regras, denominadas *rotas*, que são usadas para determinar para onde o tráfego de rede é direcionado. Toda sub-rede em uma VPC deve ser associada a uma tabela de rotas porque a tabela controla o roteamento para a sub-rede. Uma sub-rede só pode ser associada a uma única tabela de rota por vez, mas é possível associar várias sub-redes a uma mesma tabela.

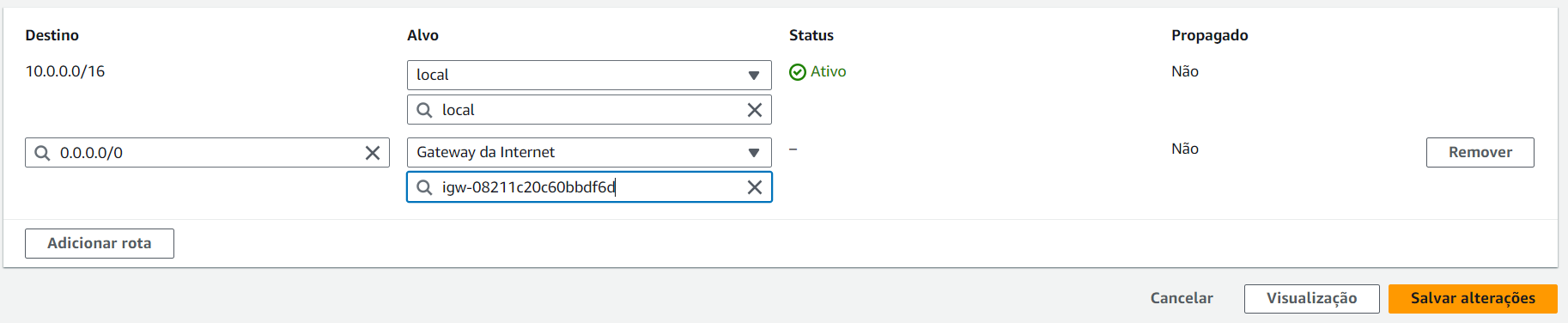
Para usar um gateway de Internet, a tabela de rota da sub-rede deve conter uma rota que direcione o tráfego vinculado à Internet para o gateway de Internet. Se uma sub-rede estiver associada a uma tabela de rota que tem uma rota para um gateway de Internet, ela será conhecida como *sub-rede pública*.

Nesta tarefa, você vai:

* Criar uma *tabela de rotas públicas* para tráfego vinculado à Internet
* Adicionar uma *rota* à tabela de rotas para direcionar o tráfego de entrada da Internet para o gateway de Internet
* Associar a sub-rede pública à nova tabela de rota

1. No painel de navegação esquerdo, selecione **Tabelas de rotas**.  
   Várias tabelas de rotas são exibidas, mas há apenas uma tabela de rota associada ao *Lab VPC*. Essa tabela de rota roteia o tráfego localmente, por isso é chamada de *tabela de rota privada*.
2. Role a tela para direita para exibir a coluna **VPC** e aumente a largura da coluna para exibir qual é usada pelo **Lab VPC**.
3. Role a página de volta para a esquerda e selecione a tabela de rota que exibe **Lab VPC**.
4. Na coluna **Nome clique no Lápis**, insira o nome Private Route Table e clique em Salvar  
      
   
5. Na parte inferior da página, selecione a guia **Rotas**.  
   Só há uma rota. Ela mostra que todo o tráfego destinado a *0.10.0.0/16* (que é o intervalo do *Lab VPC*) será roteado *localmente*. Esta rota permite que todas as sub-redes em uma VPC se comuniquem.  
   Agora, você criará uma tabela de rota pública para enviar tráfego público ao gateway de internet.
6. Selecione **Criar tabela de rotas** e defina estas configurações:
   * **Nome:** **Public Route Table**
   * **VPC:** ***Lab VPC***
   * Selecione **Criar tabela de rotas**.

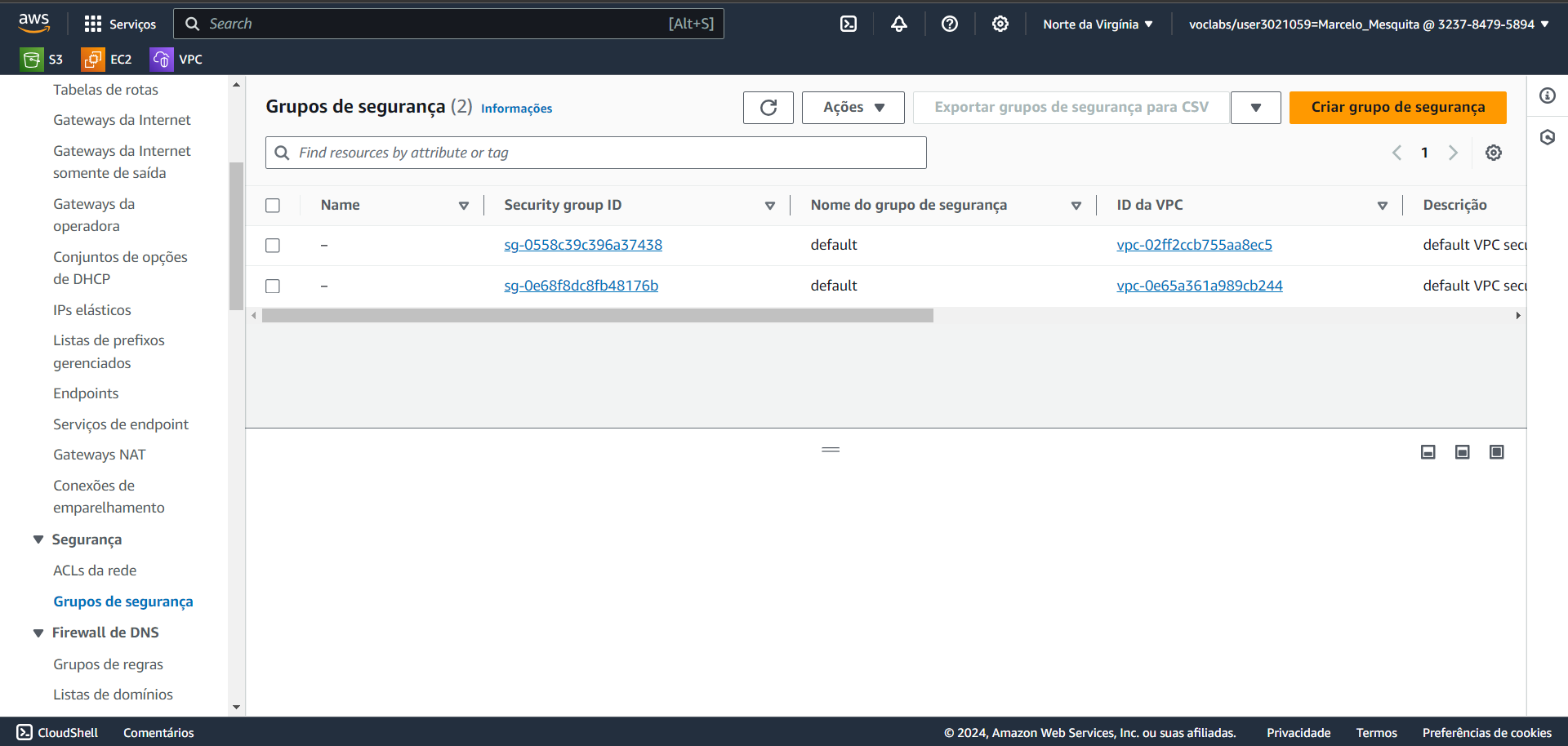
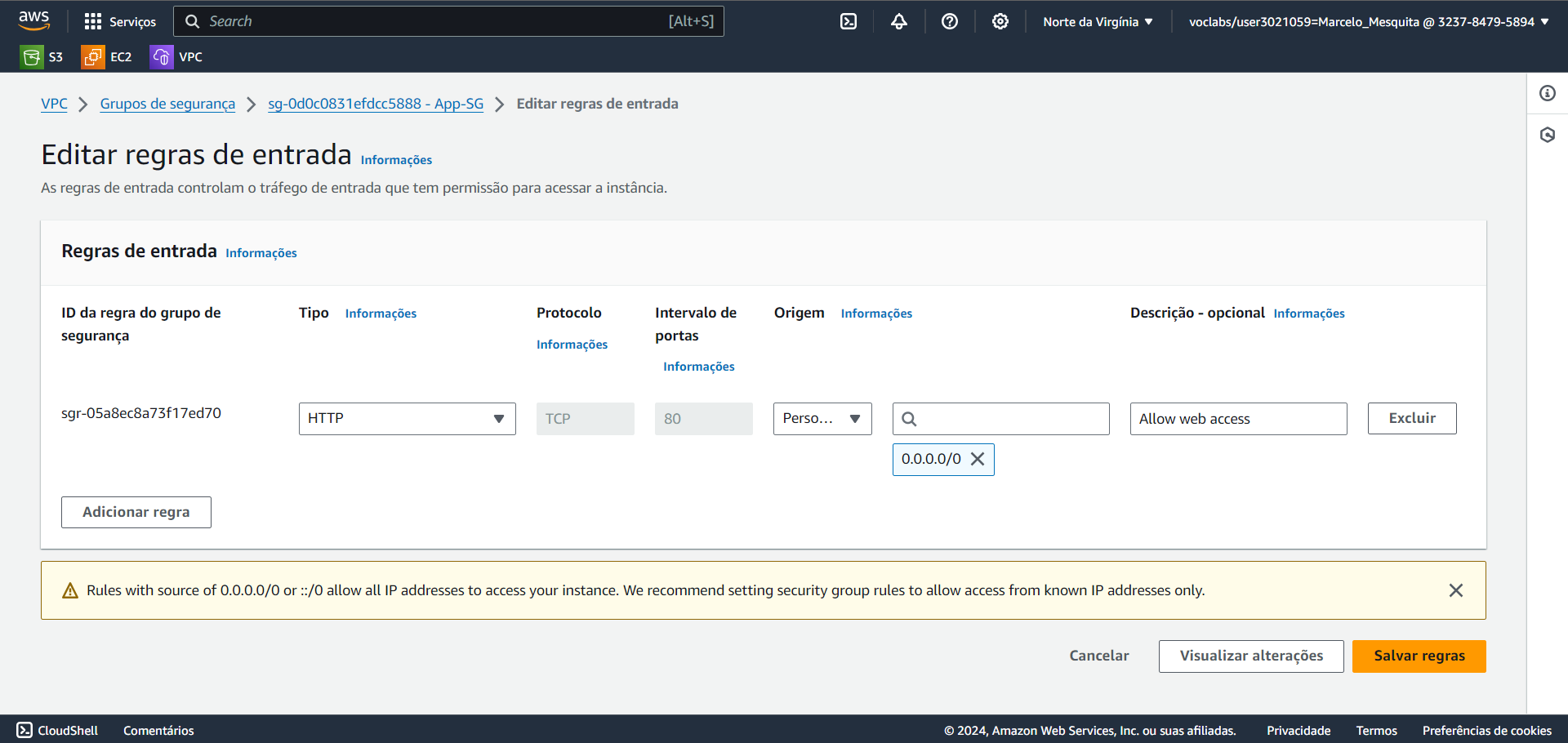
1. Na guia **Rotas**, selecione **Editar rotas**.  
   Agora você vai adicionar uma rota para direcionar o tráfego destinado à internet (*0.0.0.0/0*) ao gateway de internet.

1. Selecione **Adicionar rota** e defina estas configurações:
   * **Destino:** **0.0.0.0/0**
   * **Destino:** selecione *Gateway da Internet* e depois *Lab IGW* (IGW do laboratório) da lista.
   * Clique em **Salvar alterações**.  
       
     
2. A etapa final é *associar* essa nova tabela de rota à sub-rede pública.
3. Escolha a guia **Associações de sub-rede**.
4. Escolha **Editar associações de sub-rede**.
5. Selecione a linha com **Sub-rede pública**.( Public Subnet )
6. Escolha **Salvar associações**.  
   A sub-rede pública agora é *pública* porque tem uma entrada de tabela de rota que envia tráfego para a Internet por meio do gateway de Internet.  
   Para resumir, você pode criar uma sub-rede pública seguindo estas etapas:
   * Crie um *gateway de Internet*.
   * Crie uma *tabela de rota*.
   * Adicione uma *rota* à tabela de rota que direciona o tráfego *0.0.0.0/0* ao gateway de Internet.
   * Associe a tabela de rota a uma *sub-rede*, que se torna assim uma *sub-rede pública*.

## **Tarefa 5: criar um grupo de segurança para o servidor de aplicações**

Um *grupo de segurança* atua como um firewall virtual da instância para controlar o tráfego de entrada e saída. Os grupos de segurança operam no nível da *interface de rede elástica para a instância*. Os grupos de segurança não operam no nível de *sub-rede*. Portanto, cada instância pode ter o próprio firewall que controla o tráfego. Se você não especificar um grupo de segurança em particular no momento da execução, a instância será automaticamente atribuída ao *grupo de segurança padrão* para a VPC.

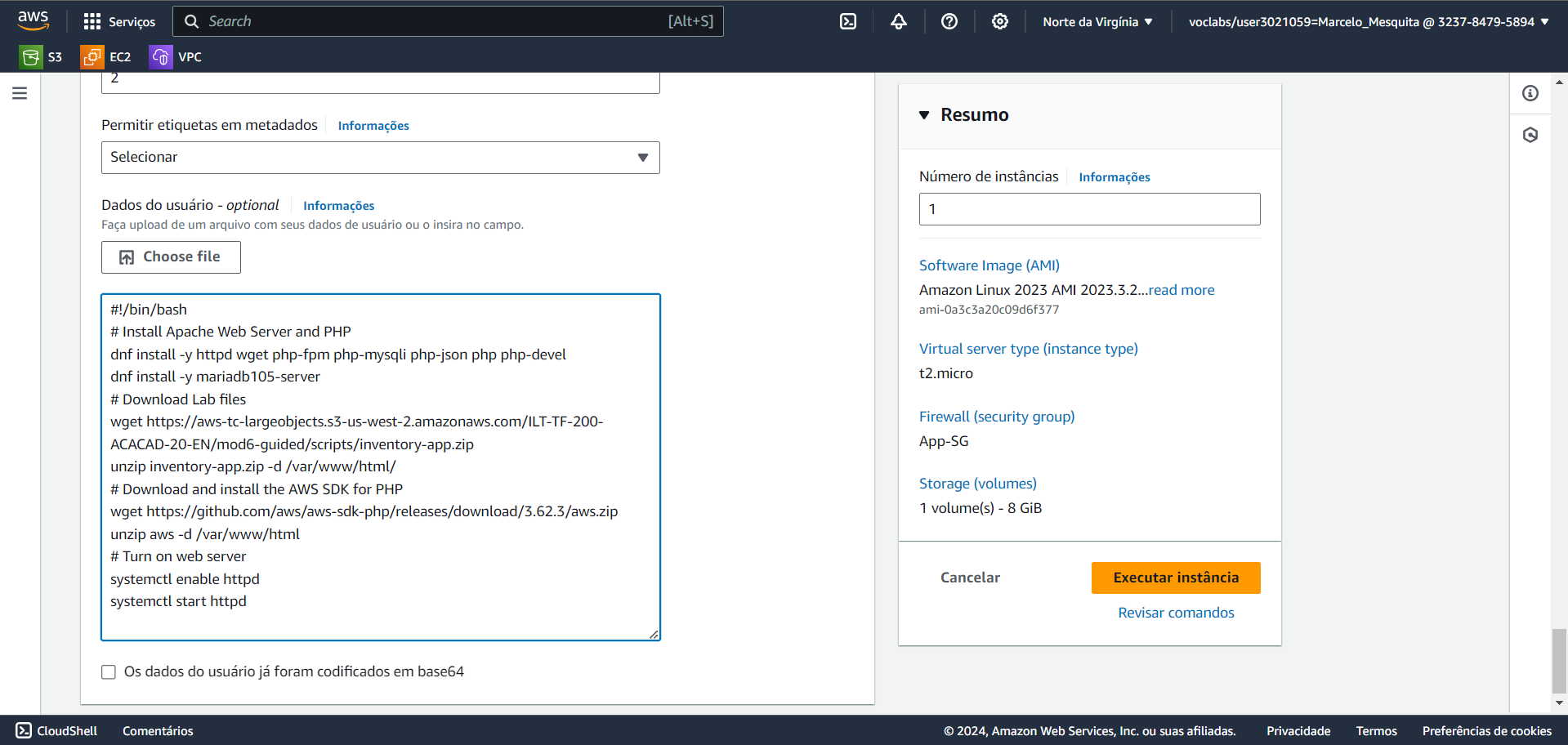
Nesta tarefa, você criará um grupo de segurança que permite que os usuários acessem o servidor de aplicações via HTTP.

1. No painel de navegação à esquerda, escolha **Grupos de segurança**.  
     
    
2. Selecione **Criar grupo de segurança** e defina estas configurações:
   * **Nome do grupo de segurança:** **App-SG**
   * **Descrição:** **Allow HTTP traffic**
   * **VPC:** Selecione ***Lab VPC***
   * Vá até a parte inferior da página e selecione **Criar grupo de segurança**.
3. Verifique se a guia **Regras de entrada** está selecionada abaixo.  
   As configurações para as **Regras de entrada** determinam qual tráfego tem permissão para chegar à instância. Você as configurará para permitir tráfego HTTP (porta 80) proveniente de qualquer lugar na Internet (*0.0.0.0/0*).
4. Selecione **Editar regras de entrada**.
5. Selecione **Adicionar regra** e defina estas configurações:
   * **Tipo:** **HTTP**
   * **Tipo de origem:** **Qualquer-IPv4**
   * **Descrição:** **Allow web access**
   * Clique em **Salvar regras**.
6. Você vai usar este **App-SG** na próxima tarefa.  
     ****

**Tarefa 6: iniciar um servidor de aplicações na sub-rede pública**

Para testar se sua VPC está configurada corretamente, você iniciará uma instância do EC2 na sub-rede pública. Você também confirmará que pode acessar a instância do EC2 pela internet.

1. Na caixa de pesquisa à direita de **Serviços**, procure e selecione **EC2** para abrir o console do EC2.
2. No menu **Executar instância**, selecione **Executar instância**. Configure estas opções:
   * **Nome**: App Server
   * Na lista de AMIs *Quick Start* disponíveis, mantenha a configuração padrão **Amazon Linux** selecionada. Também mantenha a configuração padrão específica **Amazon Linux 2023 AMI** (AMI do Amazon Linux 2023) selecionada.
   * No painel *Tipo de instância*, mantenha a configuração padrão **t2.micro** selecionada.
   * No menu **Nome do par de chaves**, selecione **sua par de Chave** .
   * Ao lado de Network settings (Configurações de rede), selecione **Editar** e configure:
     + **Rede:** ***Lab VPC***
     + **Sub-rede:** ***Publica Subnet***
   * Em Firewall (grupos de segurança), selecione **Select an existing security group** (**Selecionar um grupo de segurança existente**).
     + Para **Common security groups** (**Grupos de segurança comuns**), selecione **App-SG**.
   * Na seção *Configurar armazenamento*, mantenha a configuração padrão.
   * Expanda o painel **Detalhes avançados**.
   * **Perfil de instância do IAM:** ***LabInstanceProfile***
   * Role até a parte inferior da página, copie e cole o código mostrado abaixo na caixa **Dados do usuário**:

#!/bin/bash  
# Install Apache Web Server and PHP  
dnf install -y httpd wget php-fpm php-mysqli php-json php php-devel  
dnf install -y mariadb105-server  
# Download Lab files  
wget https://aws-tc-largeobjects.s3-us-west-2.amazonaws.com/ILT-TF-200-ACACAD-20-EN/mod6-guided/scripts/inventory-app.zip  
unzip inventory-app.zip -d /var/www/html/  
# Download and install the AWS SDK for PHP  
wget https://github.com/aws/aws-sdk-php/releases/download/3.62.3/aws.zip  
unzip aws -d /var/www/html  
# Turn on web server  
systemctl enable httpd  
systemctl start httpd  
  


* + Na parte inferior do painel **Resumo** à direita da tela, selecione **Executar instância**.  
    Uma mensagem de sucesso será exibida.

1. Selecione  **instâncias**  no Lado Esquerdo
2. Aguarde até que a instância do App Server (Servidor de aplicações) mostre *2/2 checks passed* (2/2 verificações aprovadas) na coluna **Verificação de status**.  
    Isso pode levar alguns minutos. Clique no ícone de atualização na parte superior da página a cada 30 segundos ou mais para conferir rapidamente o status mais recente da instância.
3. Selecione **App Server** (Servidor de aplicações) e clique no ID da instância.
4. Copie o valor **Public IPv4 DNS** (DNS IPv4 público).
5. Abra uma nova guia do navegador da web com esse endereço IP.  
   Se sua VPC foi configurada corretamente, você deverá ver a aplicação de inventário e a mensagem *Please configure Settings to connect to database* (Defina as configurações para se conectar ao banco de dados). Nenhuma configuração de banco de dados foi definida ainda, mas a aparência da aplicação de inventário prova que a sub-rede pública foi configurada corretamente.  
    Se a aplicação de inventário não for exibida, aguarde 60 segundos e atualize a página para tentar novamente. Pode levar alguns minutos para a instância do EC2 inicializar e executar o script que instala o software.

## **Laboratório concluído**

Parabéns! Você concluiu o laboratório.

1. Selecione Encerrar laboratório na parte superior da página e **Sim** para confirmar.  
   Um painel informa que *DELETE has been initiated… You may close this message box now* (EXCLUSÃO iniciada… Agora você pode fechar esta caixa de mensagem).
2. Clique no **X** no canto superior direito para fechar o painel.