

Crie a sua VPC e inicie um servidor web

Objetivos

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

- Criar uma nuvem privada virtual (VPC)
- Criar sub-redes
- Configurar um grupo de segurança
- Iniciar uma instância do Amazon Elastic Compute Cloud (Amazon EC2) dentro da nova VPC

Duração

O laboratório levará aproximadamente **45 minutos** para ser concluído.

Cenário

Neste laboratório, você usará a Amazon Virtual Private Cloud (VPC) para criar sua própria VPC e adicionar componentes adicionais a ela para produzir uma rede personalizada para um cliente Fortune 100. Você também cria grupos de segurança para sua instância do EC2. Em seguida, você configurará e personalizará uma instância do EC2 para executar um servidor web e iniciá-lo na VPC que parece com o seguinte diagrama do cliente:

Diagrama do cliente

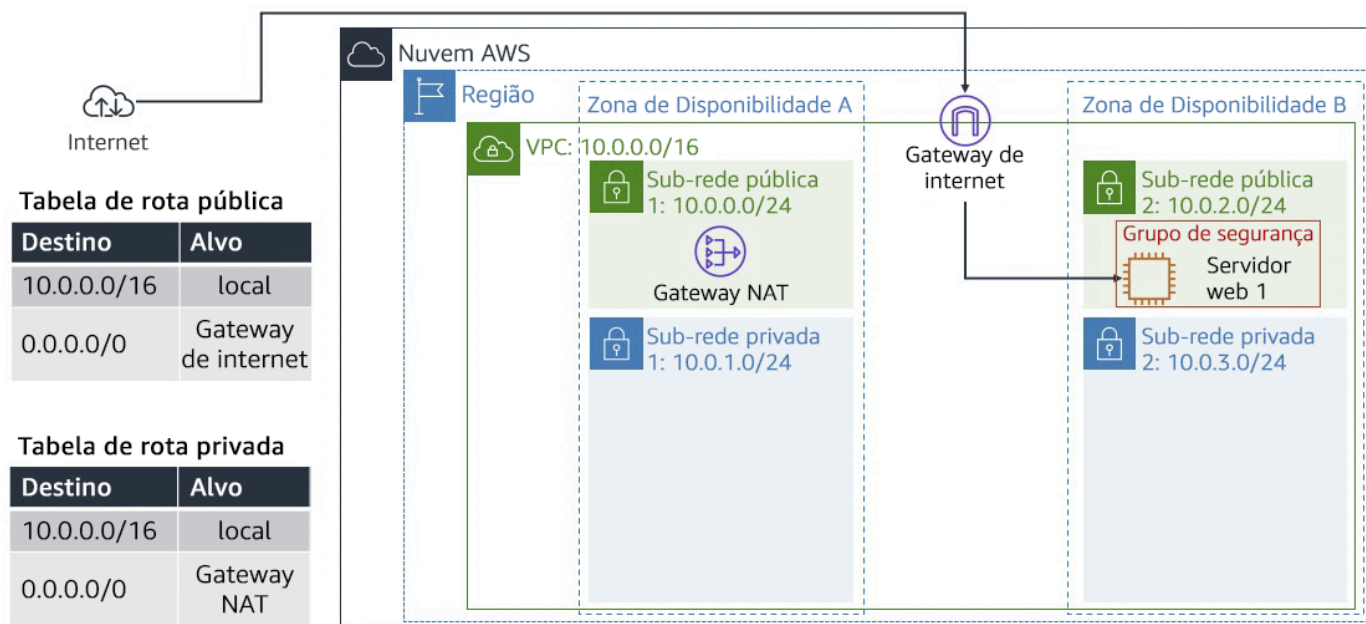


Figura: o cliente está solicitando a construção desta arquitetura para iniciar seu servidor web com êxito.

Restrições de serviço da AWS

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

Acessar o Console de Gerenciamento da AWS

1. Na parte superior destas instruções, escolha **Start Lab** (Iniciar laboratório) para iniciar este laboratório.

Um painel **Start Lab** (Iniciar laboratório) aparece, exibindo o status do laboratório.

i 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 a mensagem **Lab status: ready** (Status do laboratório: pronto) seja exibida e clique no **X** para fechar o painel **Start Lab** (Iniciar laboratório).

3. Na parte superior destas instruções, selecione **AWS**.

Esta opção abrirá o Console de Gerenciamento da AWS em uma nova guia do navegador. O sistema faz seu login automaticamente.

i Dica: se a nova guia do navegador não for aberta, um banner ou um ícone na parte superior do navegador indicará que o navegador está impedindo que o site abra janelas pop-up. Clique no banner ou no ícone e escolha **Allow pop-ups** (Permitir pop-ups).

Tarefa 1: Criar a VPC

Nesta tarefa, você usa o assistente de VPC para criar uma VPC, um gateway da internet e duas sub-redes em uma única Zona de Disponibilidade. Um gateway da Internet é um componente de VPC que permite a comunicação entre instâncias em sua VPC e a Internet.

Depois de criar uma VPC, você pode adicionar sub-redes. Cada sub-rede reside inteiramente dentro de uma zona de disponibilidade e não pode abranger zonas. Se o tráfego de uma sub-rede for roteado para um gateway da internet, a sub-rede é conhecida como sub-rede pública. Se uma sub-rede não tiver uma rota para o gateway da internet, a sub-rede será conhecida como uma sub-rede privada.

O assistente também cria um gateway NAT, que é usado para fornecer conectividade com a internet para instâncias do EC2 nas sub-redes privadas.

4. No canto superior direito destas instruções, escolha **AWS**. O Console de Gerenciamento da AWS é aberto em uma nova guia.
5. Quando você estiver no console da AWS, digite e procure por **VPC** na barra de pesquisa, na parte superior. Selecione VPC na lista.
6. Agora, você está no painel da Amazon VPC. Você usa o serviço Amazon Virtual Private Cloud (Amazon VPC) para montar a sua VPC.
7. Escolha **Criar VPC** e configure as seguintes opções:
 - **Recursos a serem criados:** escolha **VPC e muito mais**
 - **Geração automática da etiqueta de nome:** desmarque a caixa **Gerar automaticamente**.
 - **IPv4 CIDR (CIDR IPv4):** insira **10.0.0.0/16**.
 - **IPv6 CIDR block (bloco CIDR IPv6):** selecione **No IPv6 CIDR Block** (Nenhum bloco CIDR IPv6).
 - **Tenancy:** escolha **Padrão**.
 - **Número de Zonas de Disponibilidade (AZs):** **1**
 - **Número de sub-redes públicas:** **1**
 - **Número de sub-redes privadas:** **1**

- Expanda **Personalizar blocos CIDR de sub-redes**

- **Public subnet CIDR block in us-west-2a** (Bloco CIDR de sub-rede pública em us-west-2a):

10.0.0.0/24

- **Private subnet CIDR block in us-west-2a** (Bloco CIDR de sub-rede privada em us-west-2a):

10.0.1.0/24

- **Gateways NAT:** selecione **In 1 AZ** (Em 1 AZ)

- **Endpoints da VPC:** escolha **Nenhum**

8. No painel **Visualização**, dê um nome aos recursos, da seguinte forma:

- VPC: **Lab VPC**

- Subnets (2)

- Na primeira caixa, *Public subnet one without name tag* (Sub-rede pública 1 sem tag de nome):

Public Subnet 1

- Na segunda caixa, *Private subnet one without name tag* (Sub-rede privada 1 sem tag de nome):

Private Subnet 1

- Tabelas de rota (2)

- Na primeira caixa, *Public route table without name tag* (Tabela de rota pública sem tag de nome):

Public Route Table

- Na segunda caixa, *Private route table without name tag* (Tabela de rota privada sem tag de nome):

Private Route Table

9. Escolha **Criar VPC**.

Na próxima tela, uma mensagem de *Sucesso* é exibida com detalhes da VPC.

10. Selecione **Visualizar VPC**.

Os detalhes de *Lab VPC* (VPC do laboratório) são exibidos conforme a configuração.

Tarefa 2: Criar sub-redes adicionais

Nesta tarefa, você cria duas sub-redes adicionais em uma segunda Zona de Disponibilidade. Isso é útil para criar recursos em várias Zonas de Disponibilidade para fornecer alta disponibilidade.

11. No painel de navegação à esquerda, escolha **Sub-redes**.

12. Para configurar a segunda sub-rede pública, escolha **Criar sub-rede** e configure as seguintes opções:

- **VPC ID** (ID da VPC): na lista suspensa, escolha **Lab VPC** (VPC do laboratório).
- **Nome da sub-rede:** insira **Public Subnet 2**
- **Zona de disponibilidade:** Sem preferências
- **IPv4 CIDR block** (Bloco CIDR IPv4): insira **10.0.2.0/24**.

13. Selecione **Criar sub-rede**.

A sub-rede terá todos os endereços IP que começam com **10.0.2.x**.

14. Para configurar a segunda sub-rede privada, escolha **Criar sub-rede** e configure as seguintes opções:

- **VPC ID** (ID da VPC): na lista suspensa, escolha **Lab VPC** (VPC do laboratório).
- **Nome da sub-rede:** insira **Private Subnet 2**
- **Zona de disponibilidade:** Sem preferências
- **IPv4 CIDR block** (Bloco CIDR IPv4): insira **10.0.3.0/24**.

15. Selecione **Criar sub-rede**.

A sub-rede terá todos os endereços IP que começam com **10.0.3.x**.

Tarefa 3: Associar as sub-redes e adicione rotas.

16. No painel de navegação à esquerda, escolha **Tabelas de rotas**.

17. Selecione **Tabela de rotas públicas**

18. No painel inferior, escolha a guia **Associações de sub-rede**.

19. Em **Sub-redes sem associações explícitas**, escolha **Editar associações de sub-rede**.

20. Marque a caixa de seleção para **Public Subnet 2** (Sub-rede pública 2).

21. Selecione **Salvar associações**.

Agora, você configurará a tabela de rota usada pelas sub-redes privadas.

22. Selecione **Tabela de rotas privadas**.

23. No painel inferior, escolha a guia **Associações de sub-rede**.

24. Em **Sub-redes sem associações explícitas**, escolha **Editar associações de sub-rede**.

25. Marque a caixa de seleção para **Private Subnet 2** (Sub-rede privada 2).

26. Selecione **Salvar associações**.

A VPC agora tem sub-redes públicas e privadas configuradas em duas Zonas de Disponibilidade:

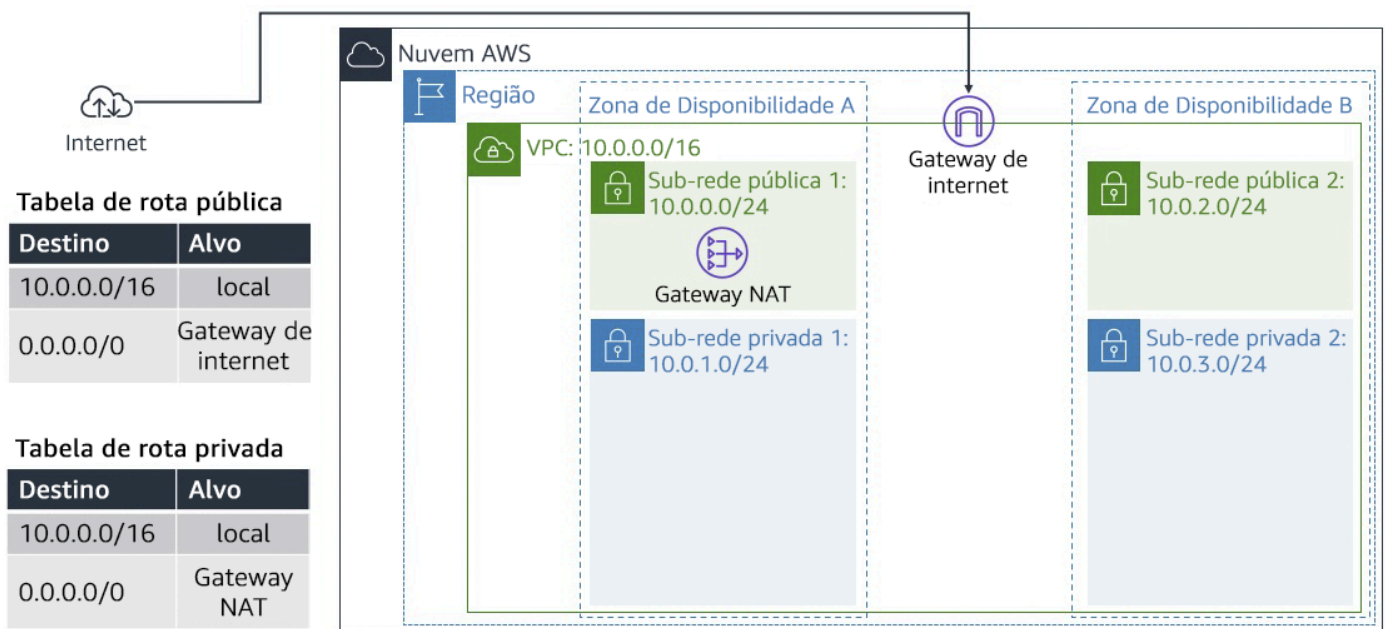


Figura: a criação dos recursos de rede e componentes de roteamento e a conexão desses recursos que tornam a VPC funcional como uma rede.

Tarefa 4: Criar um grupo de segurança da VPC

Nesta tarefa, você criará um grupo de segurança de VPC, que atuará como um firewall virtual para a instância. Ao iniciar uma instância, você pode associar um ou mais grupos de segurança à instância. Você pode adicionar regras a cada grupo de segurança que permite tráfego de entrada ou de saída nas instâncias associadas.

27. No painel de navegação à esquerda, escolha **Grupos de segurança**.

28. Selecione **Criar grupo de segurança**.

29. Configure o grupo de segurança com as seguintes opções:

- **Nome do grupo de segurança:** insira `Web Security Group`.
- **Descrição:** insira `Enable HTTP access`
- **VPC:** selecione **Lab VPC** (VPC do laboratório).

30. Em **Regras de entrada**, selecione **Adicionar regra**.

31. Configure as seguintes opções:

- **Tipo:** escolha **HTTP**.
- **Origem:** escolha **Anywhere-IPv4** (Qualquer lugar-IPv4).
- **Descrição:** insira `Permit web requests`

32. Selecione **Criar grupo de segurança**.

Você usará este grupo de segurança na próxima tarefa ao iniciar uma instância do EC2.

Tarefa 5: Iniciar uma instância de servidor web

Nesta tarefa, você iniciará uma instância do EC2 na nova VPC. Você configurará a instância para atuar como um servidor web.

33. No Console de Gerenciamento da AWS, na barra **Pesquisar**, insira `EC2` e selecione-o para acessar o **EC2 Management Console** (Console de gerenciamento do EC2).

34. No painel de navegação à esquerda, selecione **Instâncias**.

35. Escolha **Executar instâncias** e configure o seguinte:

- Na seção **Nome e tags**, **Nome:** `Web Server 1`.
- Na seção **Application and OS Images (Amazon Machine Image)** (Aplicação e imagens OS [imagem de máquina da Amazon]), configure estas opções:
 - **Início rápido:** escolha **Amazon Linux**.
 - **Imagem de máquina da Amazon (AMI):** no menu suspenso, selecione **Amazon Linux 2 AMI (HVM)**.
- Na seção **Tipo de instância**, selecione **t3.micro**.
- Na seção **Par de chaves (login)**, selecione **vockey**.



36. Na seção **Configurações de rede**, selecione **Editar** e configure estas opções:

- **VPC - *required* (VPC - obrigatório):** selecione **Lab VPC** (VPC de laboratório).
- **Sub-rede:** selecione **Sub-rede pública**.
- **Atribuir IP público automaticamente:** selecione **Habilitar**.
- **Firewall (grupos de segurança):** escolha **Selecionar grupo de segurança existente**.
 - Escolha **Web Security Group** (Grupo de segurança da web).


37. Expanda **Detalhes avançados**.

38. Em **Dados do usuário**, copie e cole o seguinte código

```
#!/bin/bash
#Install Apache Web Server and PHP
yum install -y httpd mysql php
#Download Lab files
wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-100-RESTR-1/267-lab-NF-build-vpc-web-server/s3/lab-app.zip
unzip lab-app.zip -d /var/www/html/
#Turn on web server
chkconfig httpd on
service httpd start
```

39. Escolha **Executar instância**.
40. Para exibir a instância executada, escolha **Visualizar todas as instâncias**.
41. Aguarde até que o **Web Server 1** (Servidor web 1) indique **2/2 checks passed** (2/2 verificações aprovadas) na coluna **Verificação de status**.
42.  Isso pode levar alguns minutos. Para atualizar a página, escolha Atualizar  na parte superior da página. Agora, você se conecta ao servidor web em execução na instância do EC2.
43. Marque a caixa de seleção para a instância e escolha a guia **Detalhes**.
44. Copie o valor **Public IPv4 DNS** (DNS IPv4 público).
45. Abra uma nova guia do navegador da web, cole o valor **Public IPv4 DNS** (DNS IPv4 público) e pressione Enter.

Se tudo tiver dado certo, a página deverá ter a seguinte aparência:


Load Test
RDS

Meta-Data	Value
InstanceId	i-05a488dac28dc5d0f
Availability Zone	us-west-2b

Current CPU Load: 0%

Figura: a página de sucesso de quando o servidor web é iniciado.

Veja a seguir a arquitetura completa que você implantou:

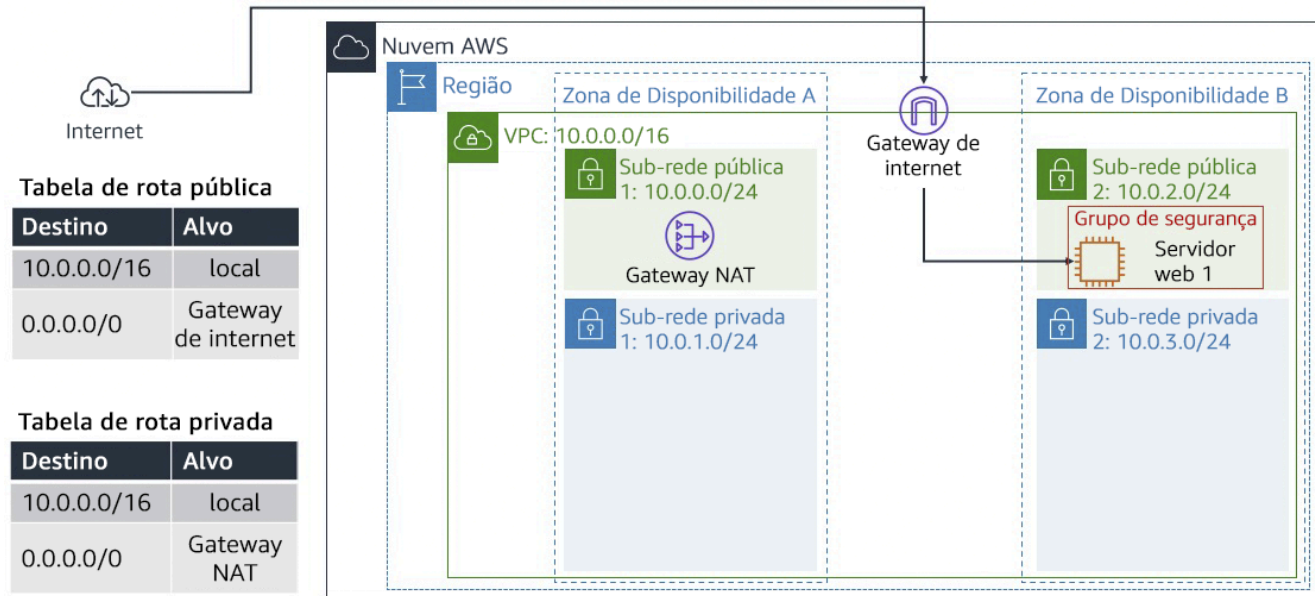


Figura: uma imagem do produto final, que é a entrega da solicitação exata do cliente: uma VPC totalmente funcional com seus recursos (rede e segurança) e um servidor web.

Recapitulação

► Neste laboratório

Recursos adicionais

- [O que é Amazon VPC?](#)

Laboratório concluído 🎓

🚩 Parabéns! Você concluiu o laboratório.

46. Na parte superior da página, selecione **End Lab** (Encerrar laboratório) e clique em **Sim** para confirmar sua decisão.

Um painel aparece indicando que **You may close this message box now. Lab resources are terminating.** (Você pode fechar esta caixa de mensagem agora. Os recursos do laboratório estão sendo interrompidos).

47. Na parte superior direita, escolha o **X** para fechar o painel **End Lab** (Encerrar laboratório).

Para obter mais informações sobre o AWS Training and Certification, consulte [AWS Training and Certification](#).

Seus comentários são sempre bem-vindos e valorizados.

Para compartilhar sugestões ou correções, forneça os detalhes em nosso [Formulário de contato do AWS Training and Certification](#).

© 2022 Amazon Web Services, Inc. e suas afiliadas. Todos os direitos reservados. Este trabalho não pode ser reproduzido nem redistribuído, parcial ou integralmente, sem a permissão prévia por escrito da Amazon Web Services, Inc. A cópia, a venda ou o empréstimo para fins comerciais é proibido.