Laboratório 3 da ACF: crie sua VPC e execute um servidor web

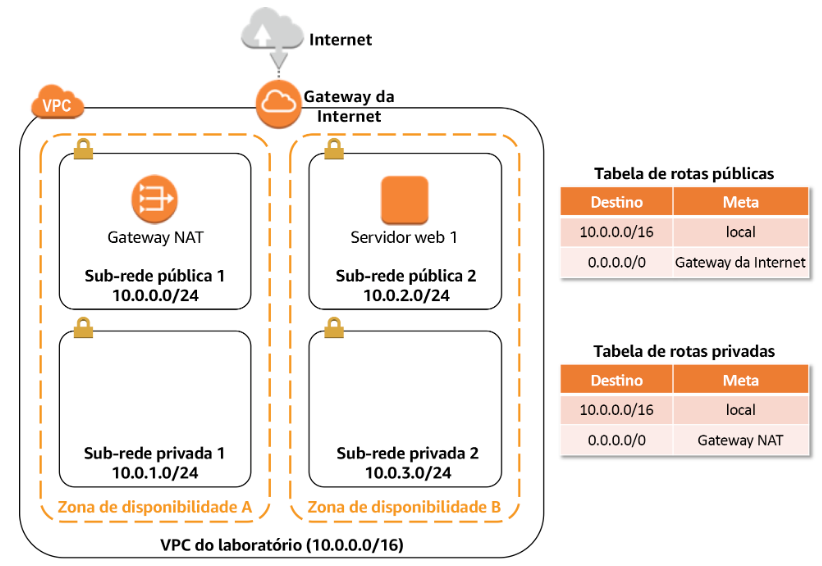
**Versão 4.6.6 (TESS1)**

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. Você também criará grupos de segurança para sua instância do EC2. Em seguida, você configurará e personalizará uma instância do EC2 para executar um servidor web e executá-lo na VPC.

**O Amazon Virtual Private Cloud (Amazon VPC)** permite executar recursos do Amazon Web Services (AWS) em uma rede virtual que você definiu. Essa rede virtual se assemelha a uma rede tradicional que você operaria no seu datacenter, com os benefícios de usar a infraestrutura escalável da AWS. Você pode criar uma VPC que abranja várias zonas de disponibilidade.

**Cenário**

Neste laboratório, você cria a seguinte infraestrutura:



**Objetivos**

Depois de concluir este laboratório, você pode:

– Criar uma VPC. – Criar sub-redes. – Configurar um grupo de segurança. – Executar uma instância do EC2 em uma VPC.

**Duração**

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

Como acessar o Console de Gerenciamento da AWS

1. Na parte superior dessas instruções, clique em Start Lab (Iniciar laboratório) para iniciar seu laboratório.

Um painel Start Lab (Iniciar laboratório) é aberto exibindo o status do laboratório.

1. Aguarde até ver a mensagem "**Lab status: ready**" (Status do laboratório: pronto) e clique no **X** para fechar o painel Start Lab (Iniciar laboratório).
2. Na parte superior dessas instruções, clique em AWS

Isso abrirá o Console de Gerenciamento da AWS em uma nova guia do navegador. O sistema fará o login automaticamente.

**Dica**: se uma nova guia do navegador não abrir, normalmente haverá um banner ou um ícone na parte superior do navegador indicando que o navegador está impedindo que o site abra janelas pop-up. Clique no banner ou ícone e escolha "Allow pop ups" (Permitir pop-ups).

1. Organize a guia do Console de Gerenciamento da AWS para que ela seja exibida junto com essas instruções. Idealmente, você poderá ver as duas guias do navegador ao mesmo tempo, para facilitar o acompanhamento das etapas do laboratório.

Tarefa 1: criar sua VPC

Nesta tarefa, você usará 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 (IGW)** 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 residi 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 será conhecida como uma *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 criará um *gateway NAT*, que é usado para fornecer conectividade com a Internet para instâncias do EC2 nas sub-redes privadas.

1. No **Console de Gerenciamento da AWS**, no menu **Services** (Serviços), clique em **VPC**.
2. Clique em **Launch VPC Wizard** (Executar assistente de VPC)
3. No painel de navegação à esquerda, clique em **VPC with Public and Private Subnets** (VPC com sub-redes pública e privada) (a segunda opção).
4. Clique em **Select** (Selecionar) e, em seguida:

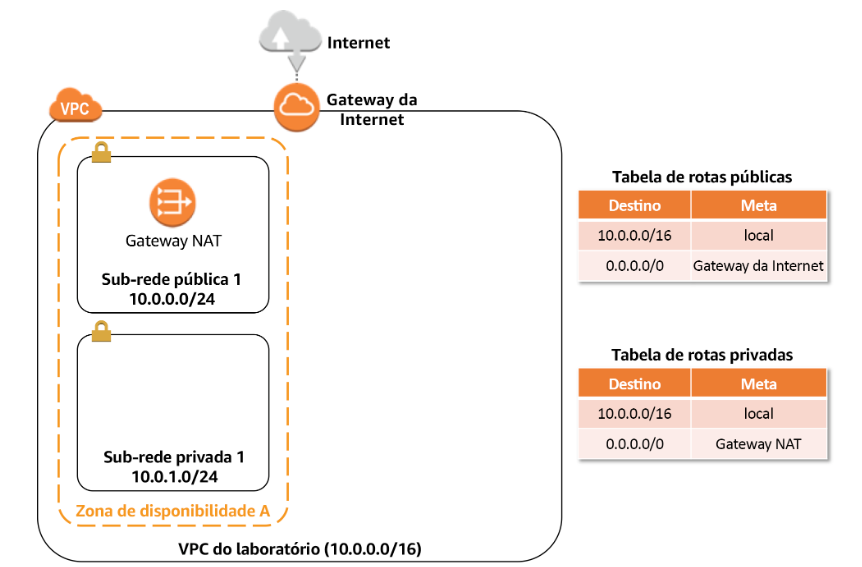
– **VPC name** (Nome da VPC): VPC do laboratório – **Availability Zone** (Zona de disponibilidade): selecione a *primeira* zona de disponibilidade – **Public subnet name** (Nome da sub-rede pública): Sub-rede pública 1 – **Availability Zone** (Zona de disponibilidade): selecione a *primeira* zona de disponibilidade a ser usada (a mesma usada acima) – **Private subnet name** (Nome da sub-rede privada): Sub-rede privada 1 – **Elastic IP Allocation ID** (ID de alocação de IP elástico): clique na caixa e selecione o endereço IP exibido

* + Clique em **Create VPC** (Criar VPC)

O assistente criará sua VPC.

1. Após a conclusão, clique em **OK**

O assistente provisionou uma VPC com uma sub-rede pública e uma sub-rede privada na mesma zona de disponibilidade, juntamente com tabelas de rotas para cada sub-rede:



A sub-rede pública tem um CIDR de**10.0.0.0/24**, o que significa que contém todos os endereços IP que começam com **10.0.0.x**.

A sub-rede privada tem um CIDR de**10.0.1.0/24**, o que significa que contém todos os endereços IP que começam com **10.0.1.x**.

Tarefa 2: criar sub-redes adicionais

Nesta tarefa, você criará 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*.

1. No painel de navegação esquerdo, clique em **Subnets** (Sub-redes).

Primeiro, você criará uma segunda sub-rede pública.

1. Clique em **Create +subnet** (Criar sub-rede) e, em seguida, configure:

– **Name tag** (Tag de nome): Sub-rede pública 2 – **VPC:** *VPC de laboratório* – ***Availability Zone****(Zona de disponibilidade): selecione a*segunda\* zona de disponibilidade – **IPv4 CIDR block** (Bloco CIDR IPv4): 10.0.2.0/24

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

1. Clique em **Create** (Criar), em seguida, **Close** (Fechar)

Agora, você criará uma segunda sub-rede privada.

1. Clique em **Create +subnet** (Criar sub-rede) e, em seguida, configure:

– **Name tag** (Tag de nome): Sub-rede privada 2 – **VPC:** *VPC de laboratório* – ***Availability Zone****(Zona de disponibilidade): selecione a*segunda\* zona de disponibilidade – **CIDR block** (Bloco CIDR): 10.0.3.0/24

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

1. Clique em **Create** (Criar), em seguida, **Close** (Fechar)

Agora, você configurará as sub-redes privadas para rotear o tráfego vinculado à Internet para o gateway NAT para que os recursos na sub-rede privada possam se conectar à Internet, sem deixar de manter os recursos privados. Isso é feito configurando uma *Tabela de rotas*.

Uma *tabela de rotas* contém um conjunto de regras, denominado *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; a tabela de rotas controla o roteamento para a sub-rede.

1. No painel de navegação esquerdo, clique em **Route Tables** (Tabelas de rotas).
2. Selecione  a tabela de rotas com **Main = Yes** (Principal = Sim) e**VPC = Lab VPC** (VPC = VPC do laboratório). (Expanda a coluna *ID de VPC*, se necessário, para visualizar o nome da VPC.)
3. No painel inferior, clique na guia **Routes** (Rotas).

Observe que **Destination 0.0.0.0/0** (Destino) está definido como **Target nat-xxxxxxxx** (Meta). Isso significa que o tráfego destinado à Internet (0.0.0.0/0) será enviado ao gateway NAT. Em seguida, o gateway NAT encaminhará o tráfego para a Internet.

Essa tabela de rotas está sendo usada para rotear o tráfego de sub-redes privadas. Agora, você adicionará um nome à tabela de rotas para facilitar o reconhecimento no futuro.

1. Na coluna **Name** (Nome) dessa tabela de rotas, clique no lápis,  em seguida, digite Private Route Table (Tabela de rotas privadas) e clique em
2. No painel inferior, clique na guia **Subnet Associations** (Associações de sub-rede).

Agora você associará essa tabela de rotas às sub-redes privadas.

1. Clique em **Edit subnet associations** (Editar associações de sub-rede)
2. Selecione  **Sub-rede privada 1** e **Sub-rede privada 2**.

 Você pode expandir a coluna *ID de sub-rede* para visualizar os nomes das sub-redes.

1. Clique em **Salvar**

Agora, você configurará a tabela de rotas usada pelas sub-redes públicas.

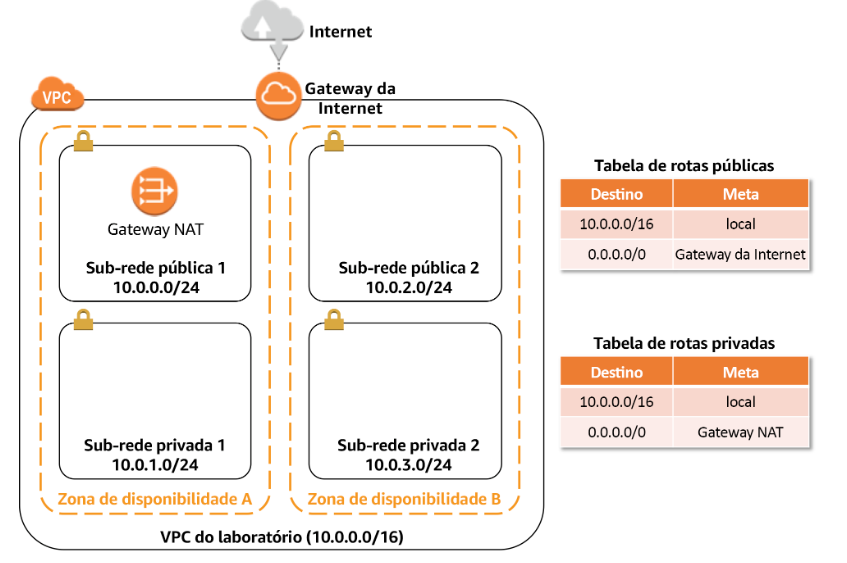
1. Selecione  a tabela de rotas com **Main = No** (Principal = Não) e**VPC = Lab VPC** (VPC = VPC do laboratório) (e desmarque quaisquer outras sub-redes).
2. Na coluna **Name** (Nome) dessa tabela de rotas, clique no lápis,  em seguida, digite Public Route Table (Tabela de rotas públicas) e clique em
3. No painel inferior, clique na guia **Routes** (Rotas).

Observe que **Destination 0.0.0.0/0** (Destino) está definido como **Target igw-xxxxxxxx** (Meta), que é o gateway da Internet. Isso significa que o tráfego vinculado à Internet será enviado diretamente para a Internet por meio do gateway da Internet.

Agora você associará essa tabela de rotas às sub-redes públicas.

1. Escolha a guia **Subnet Associations** (Associações de sub-rede).
2. Clique em **Edit subnet associations** (Editar associações de sub-rede)
3. Selecione  **Sub-rede pública 1** e **Sub-rede pública 2**.
4. Clique em **Salvar**

Sua VPC agora tem sub-redes públicas e privadas configuradas em duas zonas de disponibilidade:



Tarefa 3: criar um grupo de segurança da VPC

Nesta tarefa, você criará um grupo de segurança de VPC, que atua como um firewall virtual. Ao executar 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.

1. No painel de navegação esquerdo, clique em **Security Groups** (Grupos de segurança).
2. Clique em **Create security group** (Criar grupo de segurança) e, em seguida, configure:

– **Security group name** (Nome do grupo de segurança): grupo de segurança da Web – **Description** (Descrição): Habilitar acesso HTTP – **VPC:** *VPC de laboratório*

1. Clique em **Create** (Criar), em seguida, **Close** (Fechar)

Agora você adicionará uma regra ao grupo de segurança para permitir solicitações de entrada da Web.

1. Selecione  **Web Security Group**. (Grupo de segurança da Web).
2. Clique na guia **Inbound Rules** (Regras de entrada).
3. Clique em **Edit rules** (Editar regras)
4. Clique em **Add Rule** (Adicionar regra) e configure:

– **Type** (Tipo): *HTTP* – **Source** (Fonte): *Qualquer lugar* – **Descrição** (Description): Solicitações de permissão da Web

1. Clique em **Save rules** (Salvar regras), em seguida, **Close** (Fechar)

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

Tarefa 4: iniciar uma instância de servidor web

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

1. No menu **Services** (Serviços), clique em **EC2**.
2. Clique em **Launch Instance** (Executar instância)

Primeiro, você selecionará uma *imagem de máquina da Amazon (AMI)*, que contém o sistema operacional desejado.

1. Na linha para **Amazon Linux 2** (na parte superior), clique em **Select** (Selecionar)

O *tipo de instância* define os recursos de hardware atribuídos à instância.

1. Selecione **t2.micro** (mostrado na coluna *Type* (Tipo)).
2. Clique em **Next: Configure Instance Details** (Próximo: Configurar os detalhes da instância)

Agora, você configurará a instância para ser executada em uma sub-rede pública da nova VPC.

1. Defina estas configurações:

– **Network** (Rede): *VPC do laboratório* – **Subnet** (Sub-rede): *Sub-rede pública 2* (*não* privada) – \***Auto-assign Public IP** (Atribuir IP público automaticamente): *Habilitar*

1. Expanda a seção  **Advanced Details** (Detalhes avançados) (na parte inferior da página).
2. Copie e cole este código na caixa **User data** (Dados do usuário):
3. #!/bin/bash
4. # Install Apache Web Server and PHP
5. yum install -y httpd mysql php
6. # Download Lab files
7. wget https://aws-tc-largeobjects.s3.amazonaws.com/AWS-TC-AcademyACF/acf-lab3-vpc/lab-app.zip
8. unzip lab-app.zip -d /var/www/html/
9. # Turn on web server
10. chkconfig httpd on
11. service httpd start

Esse script será executado automaticamente quando a instância for executada pela primeira vez. O script carrega e configura um aplicativo web PHP.

1. Clique em **Next: Add Storage** (Próximo: Adicionar armazenamento)

Você usará as configurações padrão para armazenamento.

1. Clique em **Next: Add Tags** (Próximo: Adicionar tags)

As tags podem ser usadas para identificar recursos. Você usará uma tag para atribuir um nome à instância.

1. Clique em **Add Tag** (Adicionar tag) e configure:

– **Key** (Chave): Nome – **Value** (Valor): Servidor Web 1

1. Clique em **Next: Configure Security Group** (Próximo: configurar o grupo de segurança)

Você configurará a instância para usar o *grupo de segurança da Web* criado anteriormente.

1. Selecione  **Select an existing security group** (Selecionar um grupo de segurança existente)
2. Selecione  **Web Security Group**. (Grupo de segurança da Web).

Este é o grupo de segurança que você criou na tarefa anterior. Ele permitirá acesso HTTP à instância.

1. Clique em **Review and Launch** (Analisar e executar)
2. Quando solicitado com um *aviso* de que você não poderá se conectar à instância por meio da porta 22, clique em **Continue** (Continuar)
3. Revise as informações da instância e clique em **Launch** (Executar)
4. Na caixa de diálogo **Select an existing keypair** (Selecione um par de chaves existente), selecione  **I acknowledge...** (Eu reconheço...).
5. Clique em **Launch Instances** (Executar instâncias) e, em seguida, clique em **View Instances** (Visualizar instâncias)
6. Aguarde até **Servidor Web 1** mostrar *2/2 checks passed* (2/2 verificações aprovadas) na coluna**Status Checks** (Status das verificações).

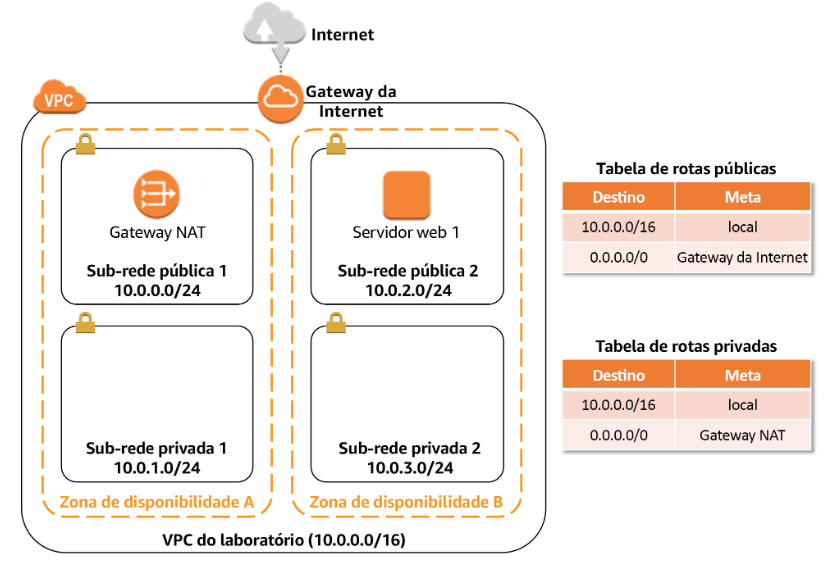
 Isso pode levar alguns minutos. Clique em Atualizar  no canto superior direito a cada 30 segundos para atualizações.

Agora, você se conectará ao servidor web em execução na instância do EC2.

1. Copie o valor **DNS Público (IPv4)** mostrado na guia **Description** (Descrição) na parte inferior da página.
2. Abra uma nova guia do navegador da Web, cole o valor **DNS Público** e pressione Enter.

Você deve ver uma página da Web exibindo o logotipo da AWS e os valores de metadados da instância.

A arquitetura completa que você implantou é:



Laboratório concluído

Parabéns! Você concluiu o laboratório.

1. Clique em End Lab (Encerrar laboratório) no topo desta página e, em seguida, clique em **Yes** (Sim) para confirmar que você deseja encerrar o laboratório.

Um painel será exibido, indicando que "DELETE has be initiated... You may close this message box now." (EXCLUIR foi iniciado... Você pode fechar esta caixa de mensagem agora)

1. Clique em **X** no canto superior direito para fechar o painel.

Envie feedback, sugestões ou correções por e-mail para: *aws-course-feedback@amazon.com*