**Build Your VPC and Launch a Web Server**

**Objectives**

After completing this lab, you should be able to:

* Create a virtual private cloud (VPC)
* Create subnets
* Configure a security group
* Launch an Amazon Elastic Compute Cloud (Amazon EC2) instance into a VPC

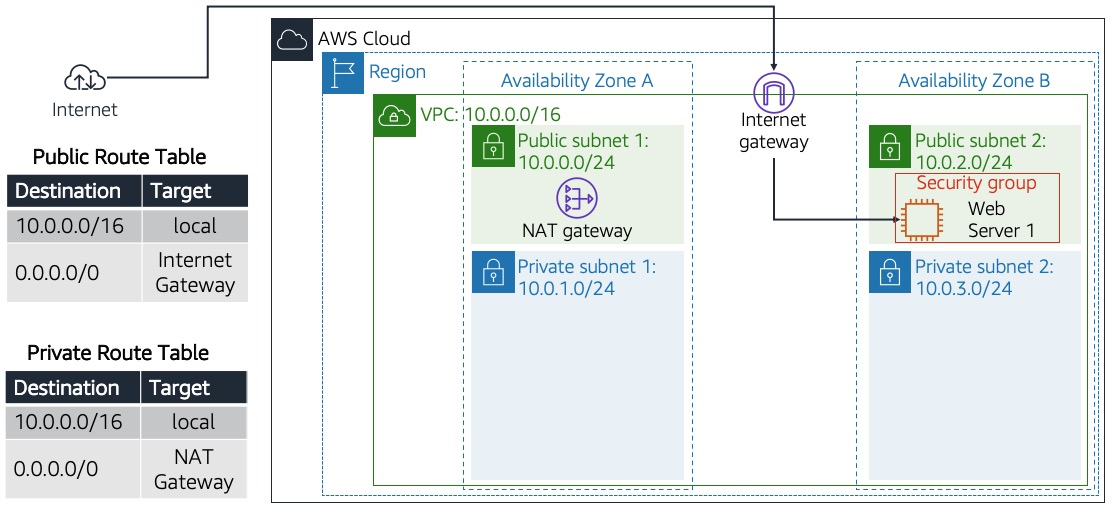
**Duration**

This lab takes approximately **45 minutes** to complete.

**Scenario**

In this lab, you use Amazon Virtual Private Cloud (VPC) to create your own VPC and add additional components to produce a customized network for a Fortune 100 customer. You also create security groups for your EC2 instance. You then configure and customize an EC2 instance to run a web server and launch it into the VPC that looks like the following customer diagram:

**Custome**

**r**

*Figure: The customer is requesting the build of this architecture to launch their web server successfully.*

**AWS service restrictions**

In this lab environment, access to AWS services and service actions might be restricted to the ones that you need to complete the lab instructions. You might encounter errors if you attempt to access other services or perform actions beyond the ones that this lab describes.

**Accessing the AWS Management Console**

1. At the top of these instructions, choose Start Lab to launch this lab.

A **Start Lab** panel opens and displays the lab status.

**Tip**: If you need more time to complete the lab, restart the timer for the environment by choosing the Start Lab button again.

1. Wait until you see the message **Lab status: ready**, and then choose the **X** to close the **Start Lab** panel.
2. At the top of these instructions, choose AWS

This option opens the AWS Management Console in a new browser tab. The system automatically signs you in.

**Tip**: If a new browser tab does not open, a banner or icon at the top of your browser will indicate that your browser is preventing the site from opening pop-up windows. Choose the banner or icon, and choose **Allow pop-ups**.

**Task 1: Create your VPC**

In this task, you use the VPC Wizard to create a VPC, an internet gateway, and two subnets in a single Availability Zone. An internet gateway is a VPC component that allows communication between instances in your VPC and the internet.

After creating a VPC, you can add subnets. Each subnet resides entirely within one Availability Zone and cannot span zones. If a subnet's traffic is routed to an internet gateway, the subnet is known as a public subnet. If a subnet does not have a route to the internet gateway, the subnet is known as a private subnet.

The wizard also creates a NAT gateway, which is used to provide internet connectivity to EC2 instances in private subnets.

1. At the upper-right of these instructions, choose **AWS**. The AWS Management Console opens in a new tab.
2. Once you are in the AWS console, type and search for VPC in the search bar at the top. Select VPC from the list.
3. You are now in the Amazon VPC dashboard. You use the Amazon Virtual Private Cloud (Amazon VPC) service to build your VPC.
4. Choose **Create VPC** and configure the following options:
   * **Resources to create:** Choose **VPC and more**
   * **Name tag auto-generation**: UnCheck the box **Auto-generate**
   * **IPv4 CIDR:** Enter 10.0.0.0/16

**IPv6 CIDR block:** Choose **No IPv6 CIDR block**.

* + **Tenancy:** Choose **Default**.
  + **Number of Availability Zones (AZs)** : **1**
  + **Number of public subnets**: **1**
  + **Number of private subnets**: **1**
  + Expand **Customize subnets CIDR blocks**
    - **Public subnet CIDR block in us-west-2a**: 10.0.0.0/24
    - **Private subnet CIDR block in us-west-2a**: 10.0.1.0/24
  + **NAT gateways**: Choose **In 1 AZ**
  + **VPC endpoints**: Choose **None**

1. On the **Preview** pane, name the resources as follows:
   * VPC: Lab VPC
   * Subnets (2)
     + First box, *Public subnet one without name tag*: Public Subnet 1
     + Second box, *Private subnet one without name tag*: Private Subnet 1
   * Route tables (2)
     + First box, *Public route table without name tag*: Public Route Table
     + Second box, *Private route table without name tag*: Private Route Table
2. Choose **Create VPC**.

On the next screen, *Success* message is displayed with VPC details.

1. Choose **View VPC**.

*Lab VPC* details are displayed as per configuration.

**Task 2: Create additional subnets**

In this task, you create two additional subnets in a second Availability Zone. This option is useful for creating resources in multiple Availability Zones to provide high availability.

1. In the left navigation pane, choose **Subnets**.
2. To configure the second public subnet, choose **Create subnet** and configure the following options:
   * **VPC ID:** From the dropdown list, choose **Lab VPC**.
   * **Subnet name:** Enter Public Subnet 2
   * **Availability Zone:** No preference
   * **IPv4 CIDR block:** Enter 10.0.2.0/24
3. Choose **Create subnet**.

The subnet will have all IP addresses starting with **10.0.2.x**.

1. To configure the second private subnet, choose **Create subnet** and configure the following options:
   * **VPC ID:** From the dropdown list, choose **Lab VPC**.
   * **Subnet name:** Enter Private Subnet 2
   * **Availability Zone:** No preference
   * **IPv4 CIDR block:** Enter 10.0.3.0/24
2. Choose **Create subnet**.

The subnet will have all IP addresses starting with **10.0.3.x**.

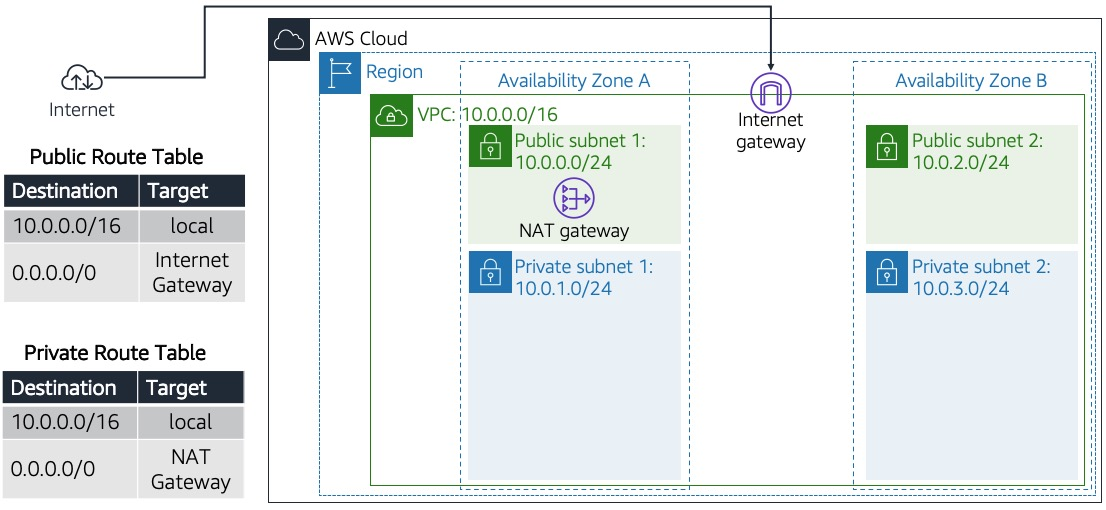
**Task 3: Associate the subnets and add routes**

1. In the left navigation pane, choose **Route Tables**.
2. Choose **Public Route Table**
3. In the lower pane, choose the **Subnet associations** tab.
4. Under **Subnets without explicit associations**, choose **Edit subnet associations**.
5. Select the check boxes for **Public Subnet 2**.
6. Choose **Save associations**.

You now configure the route table that is used by the private subnets.

1. Choose **Private Route Table**
2. In the lower pane, choose the **Subnet associations** tab.
3. Under **Subnets without explicit associations**, choose **Edit subnet associations**.
4. Select the check boxes for **Private Subnet 2**.
5. Choose **Save associations**.

Your VPC now has public and private subnets configured in two Availability Zones:



*Figure: The creation of the networking resources and routing components and attachment of these resources that make the VPC functional as a network.*

**Task 4: Create a VPC security group**

In this task, you create a VPC security group, which acts as a virtual firewall for your instance. When you launch an instance, you associate one or more security groups with the instance. You can add rules to each security group that allow traffic to or from its associated instances.

1. In the left navigation pane, choose **Security Groups**.
2. Choose **Create security group**.
3. Configure the security group with the following options:
   * **Security group name:** Enter Web Security Group
   * **Description:** Enter Enable HTTP access
   * **VPC:** Choose **Lab VPC**.
4. Under **Inbound rules**, choose **Add rule**.
5. Configure the following options:
   * **Type:** Choose **HTTP**.
   * **Source:** Choose **Anywhere IPv4**.
   * **Description:** Enter Permit web requests
6. Choose **Create security group**.

You use this security group in the next task when launching an EC2 instance.

**Task 5: Launch a web server instance**

In this task, you launch an EC2 instance into the new VPC. You configure the instance to act as a web server.

1. On the AWS Management Console, in the **Search** bar, enter and choose EC2 to go to the **EC2 Management Console**.
2. In the left navigation pane, choose **Instances**.
3. Choose **Launch instances** and configure the following options:

* In the **Name and tags** section, **Name:** Web Server 1.
* In the **Application and OS Images (Amazon Machine Image)** section, configure the following options:
  + **Quick Start:** Choose **Amazon Linux**.
  + **Amazon Machine Image (AMI):** From dropdown, Choose **Amazon Linux 2 AMI (HVM)**.
* In the **Instance type** section, choose **t3.micro**.
* In the **Key pair (login)** section, choose **vockey**.

1. In the **Network settings** section, choose Edit and configure the following options:

* **VPC - *required*:** Choose **Lab VPC**.
* **Subnet:** Choose **Public Subnet 2**.
* **Auto-assign public IP:** Choose **Enable**.
* **Firewall (security groups):** Choose **Select existing security group**.
  + Choose **Web Security Group**.

1. Expand **Advanced details**
2. Under **User data**, copy and paste the following code



#!/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-RESTRT-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

1. Choose **Launch instance**.
2. To display the launched instance, choose **View all instances**.
3. Wait until the **Web Server 1** shows **2/2 checks passed** in the **Status check** column.
4. This may take a few minutes. To update the page, choose refresh at the top of the page.

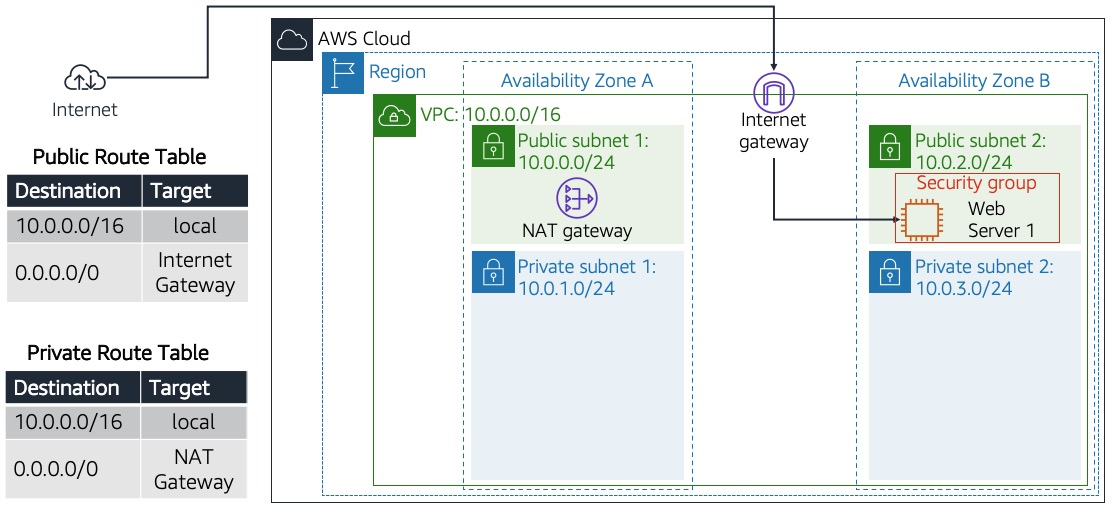
You now connect to the web server running on the EC2 instance.

1. Select the check box for the instance, and choose the **Details** tab.
2. Copy the **Public IPv4 DNS** value.
3. Open a new web browser tab, paste the **Public IPv4 DNS** value, and press Enter.

When successful, the page should look like the following:

*Figure: The success page when the web server is launched.*

The following is the complete architecture that you deployed:



*Figure: A picture of the end product, which is the delivery of the exact customer request: a fully functional VPC with its resources (network and security) and a web server.*

**Recap**

**In this lab**

**Additional resources**

* [What is Amazon VPC?](https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html)

**Lab complete**

Congratulations! You have completed the lab.

1. At the top of the page, choose **End Lab**, and then select **Yes** to confirm that you want to end the lab.

A panel appears indicating that **You may close this message box now. Lab resources are terminating ...**

1. In the upper-right corner, choose the **X** to close the **End Lab** panel.

For more information about AWS Training and Certification, see [AWS Training and Certification](https://aws.amazon.com/training/).

*Your feedback is welcome and appreciated.*

If you would like to share any suggestions or corrections, please provide the details in our [AWS Training and Certification Contact Form](https://support.aws.amazon.com/#/contacts/aws-training).

*© 2022 Amazon Web Services, Inc. and its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited.*