AWS Hands-on Workshop

Lab Guide

Build a VPC and Deploy a Web Server

Overview

In this lab session, you will use Amazon Virtual Private Cloud (VPC) to create your own VPC and add additional components to it to produce a customized network. You will create security groups for your EC2 instance. You will configure and customize the EC2 instance to run a web server and launch it into the VPC.

Objectives

After completing this lab, you will be able to:

- Create a VPC
- Create subnets
- Configure a security group
- Launch an EC2 instance into the VPC

Prerequisites

This lab requires the following:

- Access to a computer with Wi-Fi running Microsoft Windows, Mac OS X, or Linux (Ubuntu, SuSE, or Red Hat).

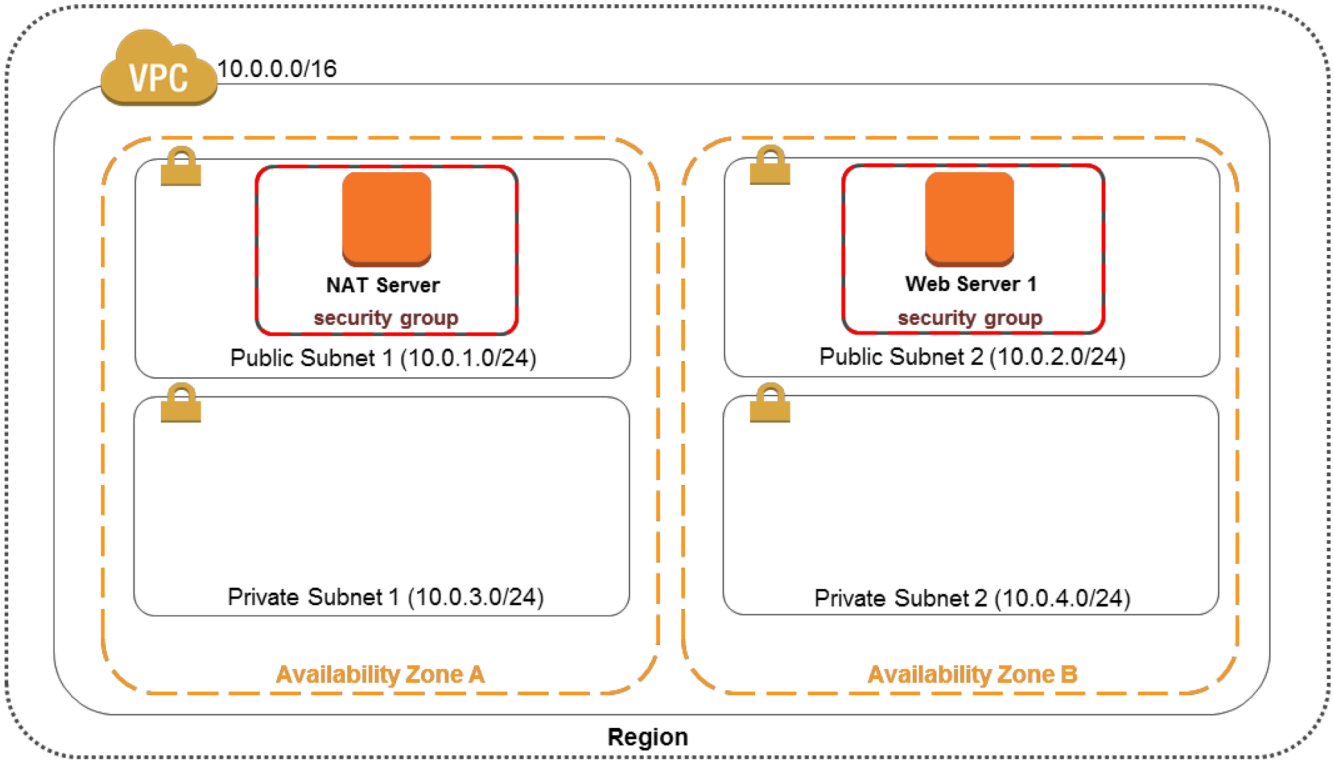
Task 1: Create Your VPC

Overview

In this section you will create your VPC.

Scenario

In this lab you will build the following infrastructure:



Task 1.1: Create Your VPC

In this task you will create a VPC with two subnets in one Availability Zone.

1.1.1 In the **AWS Management Console**, on the **Services** menu, click **VPC**.

1.1.2 Click **Start VPC Wizard**.

1.1.3 In the navigation pane, click **VPC with Public and Private Subnets**.

1.1.4 Click **Select**.

- Enter the following information:
- **IP CIDR block**: **10.0.0.0/16**
- **VPC name**: **My Lab VPC**
- **Public subnet**: **10.0.1.0/24**
- **Availability Zone**: Click an Availability Zone
- **Public subnet name**: **Public Subnet 1**
- **Private subnet**: **10.0.3.0/24**
- **Availability Zone**: Click the same Availability Zone as the Public Subnet
- **Private subnet name**: **Private Subnet 1**

1.1.5 In **Specify the details of your NAT gateway**, click **Use a NAT instance instead** on the right of the screen.

1.1.6 Select the first instance type listed in **Instance type** (example, t2.micro).

1.1.7 For **Key pair name**, select the **qwikLABS** key pair.

1.1.8 Click **Create VPC**.

1.1.9 After your VPC has been created, you will see a page stating your VPC was successfully created. Click **OK**.

Task 1.2: Create Additional Subnets

In this task you will create two additional subnets in another Availability Zone and associate the subnets with existing route tables.

1.2.1 In the navigation pane, click **Subnets**.

1.2.2 Click **Create Subnet**.

1.2.3 In the **Create Subnet** dialog box, enter the following details:

- **Name tag**: **Public Subnet 2**
- **VPC**: Click **My Lab VPC**
- **Availability Zone**: Select a different Availability Zone than you selected for Private Subnet 1 and Public Subnet 1 in the previous task.
- **CIDR block**: **10.0.2.0/24**

1.2.4 Click **Yes, Create**.

1.2.5 Click **Create Subnet**.

1.2.6 In the **Create Subnet** dialog box, enter the following details:

- **Name tag**: **Private Subnet 2**
- **VPC**: Click **My Lab VPC**
- **Availability Zone**: Select the same Availability Zone that you selected for Public Subnet 2.
- **CIDR block**: **10.0.4.0/24**

1.2.7 Click **Yes, Create**.

1.2.8 Select **Public Subnet 2**, ensure all other subnets are cleared, and then click **Route Table** in the lower pane. Scroll down and verify that the **Target** for **Destination 0.0.0.0/0** contains the prefix **igw**. If it does not, click **Edit** and click the other route table in the **Change to:** list that changes the **Target** for **Destination 0.0.0.0/0** to contain the prefix **igw**. Click **Save**.

1.2.9 Select **Private Subnet 2**, ensure all other subnets are cleared, and then click **Route Table** in the lower pane. Scroll down and verify that the **Target** for **Destination 0.0.0.0/0** contains the prefix **eni**. If it does not, click **Edit** and click the other route table in the **Change to:** list that changes the **Target** for **Destination 0.0.0.0/0** to contain the prefix **eni**. Click **Save**.

Task 1.3: Create a VPC Security Group

You will create a VPC security group that permits access for web and SSH traffic.

1.3.1 In the navigation pane, click **Security Groups**.

1.3.2 Click **Create Security Group**.

1.3.3 In the **Create Security Group** dialog box, enter the following information:

- **Name tag**: **WebSecurityGroup**
- **Group name**: **WebSecurityGroup**
- **Description**: **Enable HTTP access**
- **VPC**: Click the VPC you created in Task 1.1 (**My Lab VPC**)

1.3.4 Click **Yes, Create**.

1.3.5 Select **WebSecurityGroup**.

1.3.6 Click the **Inbound Rules** tab.

1.3.7 Click **Edit**.

1.3.8 For **Type**, click **HTTP (80)**.

1.3.9 Click in the **Source** box and type **0.0.0.0/0**

1.3.10 Click **Add another rule**.

1.3.11 For **Type**, click **SSH (22)**.

1.3.12 Click in the **Source** box and type **0.0.0.0/0**

1.3.13 Click **Save**.

Task 2: Launch Your Web Server

Overview

After you create your VPC, you will launch an EC2 instance into it and bootstrap it to act as a web server.

Command Reference File

Use the command reference file when copying text provided in this lab manual.

You should not copy and paste commands directly from this lab manual, because the manual's rich formatting may inject characters that could introduce errors to your lab experience.

Task 2.1: Launch Your First Web Server Instance

This task walks you through launching an EC2 instance into your VPC. This instance will act as your web server.

2.1.1 On the **Services** menu, click **EC2**.

2.1.2 Click **Launch Instance**.

2.1.3 In the row for **Amazon Linux AMI**, click **Select**.

2.1.4 On **Step 2: Choose an Instance Type** page, make sure **t2.micro** is selected and click **Next: Configure Instance Details**.

2.1.5 On **Step 3: Configure Instance Details** page, enter the following information and leave all other values with their default:

- **Network**: Click the VPC that you created in Task 1.1 (**My Lab VPC**).
- **Subnet**: Click **Public Subnet 2 (10.0.2.0/24)** you created in Task 1.2.
- **Auto-assign Public IP**: Click **Enable**

2.1.6 Scroll down and expand the **Advanced Details** section.

2.1.7 Copy the following user data from the command reference file and paste it into the **User data** box, ensuring **As text** is selected:

```
#!/bin/bash -ex

yum -y update

yum -y install httpd php mysql php-mysql

chkconfig httpd on

/etc/init.d/httpd start

if [ ! -f /var/www/html/lab2-app.tar.gz ]; then

cd /var/www/html

wget https://us-west-2-aws-staging.s3.amazonaws.com/awsu-ilt/AWS-100-ESS/v4.0/lab-2-configure-website-datastore/scripts/lab2-app.tar.gz

tar xvfz lab2-app.tar.gz

chown apache:root /var/www/html/lab2-app/rds.conf.php

fi
```

2.1.8 Click **Next: Add Storage**.

2.1.9 Click **Next: Tag Instance**.

2.1.10 On **Step 5: Tag Instance** page, enter the following information:

- **Key**: **Name**
- **Value**: **Web Server 1**

2.1.11 Click **Next: Configure Security Group**.

2.1.12 On **Step 6: Configure Security Group** page, click **Select an existing security group** and then select the security group you created in Task 1.3 (**WebSecurityGroup)**.

2.1.13 Click **Review and Launch**.

2.1.14 Review the instance information and click **Launch**.

2.1.15 Click **Choose an existing key pair,** click the **qwikLABS** key pair, select the acknowledgement check box, and then click **Launch Instances**.

2.1.16 Scroll down and click **View Instances**.

2.1.17 You will see two instances – **Web Server 1** and the NAT instance launched by the VPC Wizard.

2.1.18 Wait until **Web Server 1** shows *2/2 checks passed* in the **Status Checks** column. This will take 3-5 minutes. Use the refresh icon at the top right to check for updates.

2.1.19 Select **Web Server 1** and copy the **Public DNS** value.

2.1.20 Paste the **Public DNS** value in a new web browser window or tab and press Enter. You will see the **Amazon Linux AMI Test Page**.

Lab Complete

Congratulations! You have successfully completed creating a VPC and launching an EC2 instance into it.

Corrections or feedback on the course, please email us at:
aws-course-feedback@amazon.com.
For all other questions, contact us at:
https://aws.amazon.com/contact-us/aws-training/.