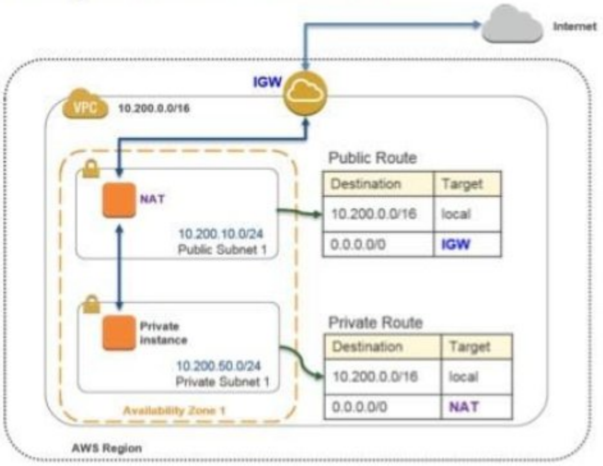
Lab 2: Creating Your First Virtual Private Cloud

Overview

In this lab, you will create a basic virtual private cloud (VPC) and extend it to produce a customized network.



Public Route

Destination	Target
10.200.0.0/16	local
0.0.0.0/0	IGW

Private Route

Destination	Target
10.200.0.0/16	local
0.0.0.0/0	NAT

Objectives

After completing this lab, you will be able to:

- Create a virtual private cloud (VPC).
- Create subnets within an Availability Zone.
- Create a Network Address Translation (NAT) instance
- Attach an Internet gateway (IGW) to your VPC.
- Create route tables.

Pre-requisites	This lab requires: • Access to a notebook computer with Wi-Fi running Microsoft Windows, Mac OS X, or Linux (Ubuntu, SuSE, or Red Hat). ○ **Note** The qwikLABS lab environment is not accessible using an iPad or tablet device, but you can use these devices to access the student guide. • For Microsoft Windows users: Administrator access to the computer. • An Internet browser such as Chrome, Firefox, or Internet Explorer 9 (previous versions of Internet Explorer are not supported). • An SSH client, such as PuTTY.

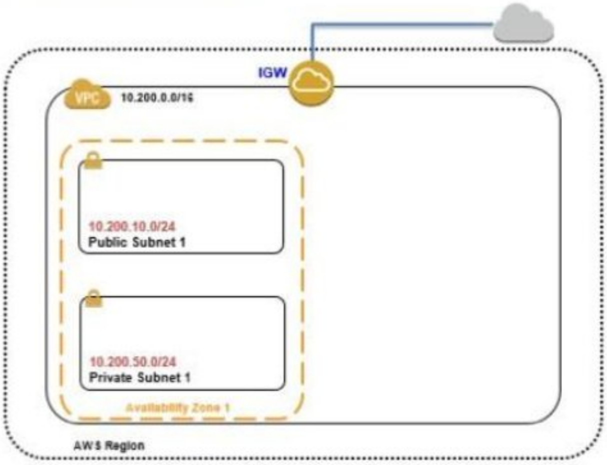
Duration	This lab will require around **40 minutes** to complete.

Task 1: Creating the Base VPC

Overview

When you first sign in to the AWS Management Console and launch **VPC Dashboard**, you will notice that there is an existing VPC; this is the default VPC. A **default VPC** is a logically isolated virtual network in the AWS cloud that is automatically created for your AWS account the first time you provision Amazon EC2 resources. When you launch an instance without specifying a subnet ID, your instance will be launched in your default VPC.

In this part of the lab, you will create a VPC with subnets and a user-specified IP address range.



Task 1-1: Create your VPC	
Overview	In this section of the lab, you will create your VPC.

Step	Instruction
1.1.1	In the **AWS Management Console**, click **VPC**. **Note** You can select your desired region from the drop-down list on the navigation bar. For now, let it remain as the default.
1.1.2	In the **VPC Dashboard** pane, click **Your VPCs**.
1.1.3	Click **Create VPC**.
1.1.4	In the **Create VPC** dialog box provide the following settings: • **Name tag:** LabVPC • **CIDR block:** 10.200.0.0/16 • **Tenancy:** Default
1.1.5	Click **Yes, Create**. You should see a new VPC named **LabVPC** with a **VPC ID** assigned to it (e.g., *vpc-530de336*).

Task 1-2: Attach an Internet gateway	
Overview	In this section of the lab, you will create an Internet gateway and attach it to your VPC so that your VPC will be accessible via the Internet.

Step	Instruction
1.2.1	In the **VPC Dashboard** pane, click **Internet Gateways**.
1.2.2	Click **Create Internet Gateway**.
1.2.3	In the **Name tag** box, type **LabVPCGateway**
1.2.4	Click **Yes, Create**. **Result** At this point, the newly created **LabVPCGateway** is not attached to your VPC. Note the ID (e.g., *igw-912a31f3*).
1.2.5	If it is not already selected, select the newly created **LabVPCGateway**, and then click **Attach to VPC**.
1.2.6	In the **Attach to VPC** dialog box, in the **VPC** drop-down list, select the **LabVPC** that you created in **Task 2.1**.
1.2.7	Click **Yes, Attach**. The **State** for the **Lab VPC Gateway** should be changed to *attached*, and the VPC ID in the **VPC** column should match your **Lab VPC**.

Task 2: Creating Subnets

Overview

You have complete control over your virtual networking environment, including selection of your own IP address range and subnets. A subnet is a segment of a VPC's IP address range where you can place groups of isolated resources.

In this task, you are going to configure your VPC so that it:

- Spans two Availability Zones (AZs) so you can distribute applications across these zones to architect for application durability and availability.
- Includes two subnets within each Availability Zone (AZ). Public subnets can route directly to the Internet. Private subnets can communicate with any other subnet within the VPC, but there is no direct access between private subnets and the Internet.

Task 2-1: Create subnets in your VPC	
Overview	In this section of the lab you will create two subnets within your VPC.

Step	Instruction
2.1.1	In the **VPC Dashboard** pane, click **Subnets**.
2.1.2	Click **Create Subnet**.
2.1.3	In the **Create Subnet** dialog box: • **Name tag:** PublicSubnet1 • **VPC:** Select the VPC that includes the name LabVPC. • **Availability Zone:** Select the first AZ (e.g., *us-west-2a*). • **CIDR block:** 10.200.10.0/24
2.1.4	Click **Yes, Create**. You should be able to see **PublicSubnet1** listed in the table.
2.1.5	Repeat steps **2.1.2** and **2.1.3** to create another subnet with the following configuration: • **Name tag:** PrivateSubnet1 • **VPC:** LabVPC • **Availability Zone**: Select the same AZ as for **PublicSubnet1**, which was the first AZ listed (e.g., *us-west-2a*). • **CIDR block:** 10.200.50.0/24
2.1.6	Click **Yes, Create**.

Task 3: Configuring Route Tables

Overview

A route table contains a set of rules called routes that are used to determine where network traffic is directed. Each subnet in your VPC must be associated with a route table; the table controls the routing for the subnet. A subnet can be associated with only one route table at a time, but you can associate multiple subnets with the same route table.

When you create a VPC, it automatically has a main route table. Initially, the main route table contains only a single route: a local route that enables communication within the VPC. If you don't explicitly associate a subnet with a route table, the subnet is implicitly associated with the main route table.

Task 3-1: Configure a route table	
Overview	In this section of the lab, you will create a route table that allows incoming and outgoing traffic through the Internet gateway you created earlier.

Step	Instruction
3.1.1	In the **VPC Dashboard** pane, click **Route Tables**.
3.1.2	Click **Create Route Table**.
3.1.3	In the **Create Route Table** dialog box: • **Name tag:** PublicRoute • **VPC:** LabVPC
3.1.4	Click **Yes, Create**.
3.1.5	If it is not already selected, select the **PublicRoute** route table you just created, and then click the **Routes** tab in the lower pane of the console.
3.1.6	Click **Edit**.
3.1.7	Click **Add another route**.
3.1.8	In the **Destination** box, type **0.0.0.0/0** Click in the **Target** box, and then select the **LabVPCGateway** that you created earlier (the ID starts with *igw-*).
3.1.9	Click **Save**.

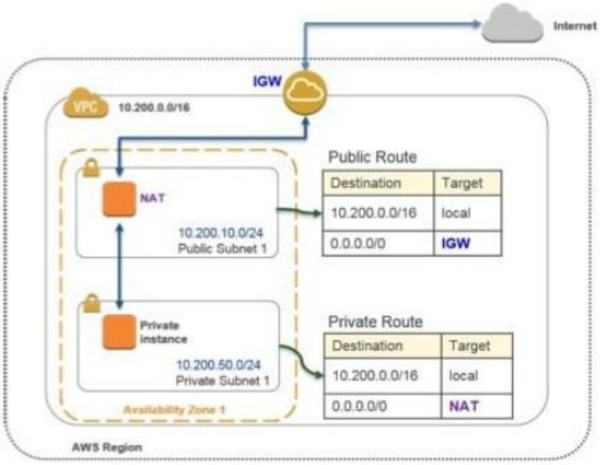
Task 3-2: Associate the route table with subnets	
Overview	In this section of the lab, you will associate your public route table and your public subnet, as well as create and configure a private route table.

Step	**Instruction**
3.2.1	With **PublicRoute** still selected, click the **Subnet Associations** tab.
3.2.2	Click **Edit**.
3.2.3	Select the check box for **PublicSubnet1** (**CIDR** range of **10.200.10.0/24**).
3.2.4	Click **Save**.
3.2.5	Click **Create Route Table**.
3.2.6	In the **Create Route Table** dialog box: • **Name tag:** PrivateRoute • **VPC:** LabVPC
3.2.7	Click **Yes, Create**.
3.2.8	With **PrivateRoute** selected, click the **Subnet Associations** tab if it is not already selected. **Note** Your **PrivateSubnet1** is associated with the **Main** route table by default.
3.2.9	Click **Edit**.
3.2.10	Select the check box for **PrivateSubnet1** (**CIDR** range of **10.200.50.0/24**).
3.2.11	Click **Save**.

Task 4: Creating a NAT Instance and a Private Instance

Overview

In this part of the lab, you will create a **Network Address Translation (NAT)** server that allows servers in the private subnet to initiate outbound connections to the Internet to download software and access Internet services such as Amazon S3. It does not allow systems on the Internet to initiate inbound connections to servers in the private subnet. The Public IP address assigned to the NAT server allows it to communicate with the Internet.



Public Route

Destination	Target
10.200.0.0/16	local
0.0.0.0/0	IGW

Private Route

Destination	Target
10.200.0.0/16	local
0.0.0.0/0	NAT

The route table sends the traffic from the instances in the private subnet to the NAT instance in the public subnet. The NAT instance sends the traffic to the Internet Gateway for the VPC.

Task 4-1: Create a NAT instance	
Overview	In this section of the lab, you will create a NAT instance in PublicSubnet1.

Step	**Instruction**
4.1.1	On the **Services** menu, click **EC2**.
4.1.2	Click **Launch Instance**.
4.1.3	To launch a new instance, you first need to select an Amazon Machine Image (AMI), which is a preconfigured template for an instance in the cloud. From the **Quick Start** menu, in the row for the first **Amazon Linux AMI**, click **Select**.
4.1.4	On the **Choose an Instance Type** page, you can select the family for your image, which determines how much RAM, storage, and processing speed your instance will have. To accept the default (**t2.micro**), click **Next: Configure Instance Details**.
4.1.5	On the **Configure Instance Details** page, make these selections: • **Network:** LabVPC • **Subnet:** PublicSubnet1 • **Auto-assign Public IP:** Enable

4.1.6	Click **Advanced Details** to expand it. Copy the contents of the user data script given below from the associated command reference file for this lab, and paste the script into the **User data** box.
	`#!/bin/sh`
	`echo 1 > /proc/sys/net/ipv4/ip_forward`
	`echo 0 >`
	`  /proc/sys/net/ipv4/conf/eth0`
	`    /send_redirects`
	`  /sbin/iptables -t nat -A POSTROUTING`
	`    -o eth0 -s 0.0.0.0/0 -j MASQUERADE`
	`/sbin/iptables-save >`
	`  /etc/sysconfig/iptables`
	`mkdir -p /etc/sysctl.d/`
	`cat <<EOF > /etc/sysctl.d/nat.conf`
	`net.ipv4.ip_forward = 1`
	`net.ipv4.conf.eth0.send_redirects = 0`
	`EOF`
	This Linux shell script configures your server as a NAT server by enabling IP forwarding on the machine and by enabling IP masquerading so that the NAT server can make external requests on behalf of internal servers.

4.1.7	Click **Next: Add Storage**.
4.1.8	Click **Next: Tag Instance**. You won't be using the storage on this instance, so you are leaving the instance's storage settings as their default.
4.1.9	In the **Value** box, type **NAT**
4.1.10	Click **Next: Configure Security Group**.
4.1.11	For **Assign a security group**, the **Create a new security group** option should be selected. • **Security group name**: NATSG • **Description:** NAT Security Group
4.1.12	Click **Add Rule**. • In the **Type** drop-down list, select **All traffic**. • In the **Source** drop-down list, select **Anywhere**.
4.1.13	Click **Review and Launch**.
4.1.14	Review the settings and then click **Launch**.
4.1.15	When prompted, accept the qwikLABS keypair, select the acknowledgement check box, and then click **Launch Instances**.
4.1.16	Click **View Instances**.

4.1.17	Select the **NAT** server you just created.
4.1.18	In the **Actions** drop-down list, point over **Networking**, and in the **Networking** drop-down list, click **Change Source/Dest. Check**.
4.1.19	On the **Enable Source/Destination Check** dialog box, click **Yes, Disable**.

Task 4-2: Add NAT to the Private Route table	
Overview	In this section of the lab, you will edit the settings of your private route table to send Internet-bound traffic to your NAT.

Step	Instruction
4.2.1	On the **Services** menu, click **VPC**.
4.2.2	In the **VPC Dashboard** pane, click **Route Tables**.
4.2.3	Select **PrivateRoute** from the list, and then click the **Routes** tab in the lower pane. There should be only one entry for **local**.
4.2.4	Click **Edit**.
4.2.5	Click **Add another route**. Provide the following settings: • In the **Destination** box, type **0.0.0.0/0** • In the **Target** box, type **NAT** to point to the instance that you created earlier, and then select it.
4.2.6	Click **Save**.

Task 4-3: Create a Private EC2 Instance	
Overview	In this section of the lab, you will create an EC2 instance and place it in your private subnet.

Step	**Instruction**
4.3.1	On the **Services** menu, click **EC2**.
4.3.2	Click **Launch Instance**.
4.3.3	From the **Quick Start** menu, in the row for the first **Amazon Linux AMI**, click **Select**.
4.3.4	To accept the default (**t2.micro**), click **Next: Configure Instance Details**.
4.3.5	On the **Configure Instance Details** page, make these selections: • **Network:** LabVPC • **Subnet:** PrivateSubnet1 • **Auto-assign Public IP:** Disable
4.3.6	Click **Next: Add Storage**.
4.3.7	Accept the default, and click **Next: Tag Instance**.
4.3.8	In the **Value** box, type **Private Instance**
4.3.9	Click **Next: Configure Security Group**.
4.3.10	For **Assign a security group**, the **Create a new security group** option should be selected. • **Security group name:** PrivateEC2 • **Description:** Private EC2 instance security group
4.3.11	There should already be an **SSH** rule. • In the **Source** drop-down list, select **Custom IP**. • In the box to the right of **Custom IP**, type **sg** A list of your security groups will appear. Select the **NATSG** security group from the list.
4.3.12	Click **Review and Launch**.

4.3.13	Review the settings and then click **Launch**.
4.3.14	When prompted, accept the qwikLABS key pair, select the acknowledgement check box, and then click **Launch Instances**.
4.3.15	Click **View Instances**.
4.3.16	Select the **NAT** instance.
4.3.17	From the **Description** tab, note the **Public IP** of the instance. Wait for the **Private Instance** to reach **Instance State:** running and **Status Checks:** 2/2 checks passed.
4.3.18	Select the instance named **Private Instance**.
4.3.19	From the **Description** tab, note the **Private IP** of the instance.

Task 5: Connecting to Your NAT Instance

Overview	In this part of the lab, you will connect to the NAT instance that you launched earlier.

Task 5-1: Download your key pair	
Overview	In this section of the lab, you will download your key pair file which was generated by qwikLABS.

Step	Instruction
5.1.1	Return to the qwikLABS web page and click the **Download PEM/PPK** drop-down list. • Windows users: click **Download PPK**. • Mac/Linux users: click **Download PEM**.
5.1.2	Save the file to the directory of your choice.