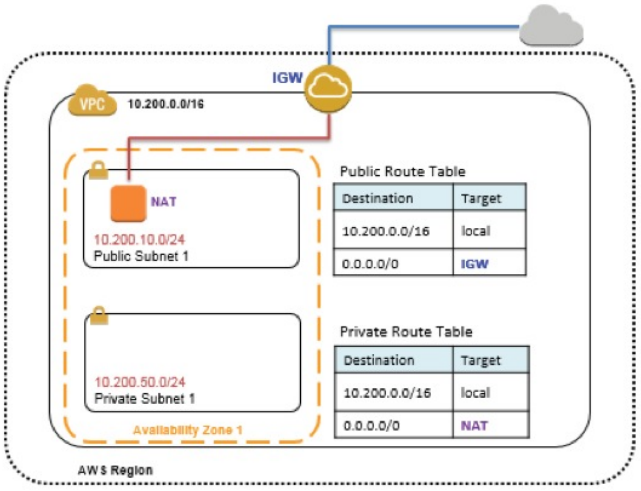
PRINTED BY: gleung@datapipe.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Lab 2: Creating Your First Virtual Private Cloud

Lab Overview

Introduction

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



Allotted time

The allotted time for this lab is listed as follows:

Component	Time
Overview	1 minute
Lab	40 minutes
Total:	**41 minutes**

Continued on next page

© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.

PRINTED BY: gleung@datapipe.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Lab Overview, Continued

Prerequisites

This lab requires:

- Access to a notebook computer with Wi-Fi on a Microsoft Windows, Mac OS X, or Linux (Ubuntu, SuSE, or Red Hat) system
  - The qwikLABS lab environment is not accessible on an iPad or tablet device, but you may use these devices to access the student guide (PDF)
- For Microsoft Windows users: Administrator access to the computer
- An Internet browser such as Chrome, Firefox, or IE9 (previous versions of Internet Explorer are not supported)
- An SSH client such as PuTTY

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.

© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.

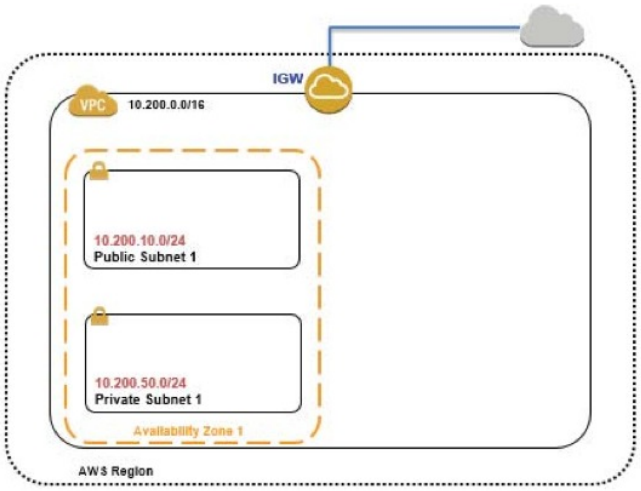
PRINTED BY: gleung@datapipe.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Creating the Base VPC

Introduction

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.



Continued on next page

© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.

PRINTED BY: gleung@datapipe.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Creating the Base VPC, Continued

Task 2.1: Create your VPC

To create your VPC:

Step	Action
2.1.1	In the AWS Management Console, on the **Services** menu, 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.
2.1.2	In the navigation pane, click **Your VPCs**.
2.1.3	Click **Create VPC**.
2.1.4	In the Create VPC dialog box: • In the **Name tag** box, type **Lab VPC** • In the **CIDR block** box, type **10.200.0.0/16** • Leave the **Tenancy** value as **Default.**
2.1.5	Click **Yes, Create**. You should see a new VPC named **Lab VPC** with a VPC ID assigned to it (e.g., *vpc-530de336*).

Task 2.2: Attach an Internet gateway

To attach an Internet gateway to your new VPC:

Step	Action
2.2.1	In the navigation pane, click **Internet Gateways**.
2.2.2	Click **Create Internet Gateway**.
2.2.3	In the **Name tag** box, type **Lab VPC Gateway**
2.2.4	Click **Yes, Create**. **Result** At this point, the newly created **Lab VPC Gateway** is not attached to your VPC. Note the ID (e.g., *igw-912a31f3*).
2.2.5	Select the newly created **Lab VPC Gateway**, and then click **Attach to VPC**.
2.2.6	In the Attach to VPC dialog box, select the **Lab VPC** that you created in Task 2.1.
2.2.7	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**.

© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.

PRINTED BY: gleung@datapipe.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Creating Subnets

Introduction

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 2.3: Create subnets in your VPC

To create subnets inside your VPC:

Step	Action
2.3.1	In the navigation pane, click **Subnets**.
2.3.2	Click **Create Subnet**.
2.3.3	In the **Create Subnet** dialog box: • In the **Name tag** box, type **Public Subnet 1** • For **VPC**, click **Lab VPC** (10.200.0.0|Lab VPC). • For **Availability Zone**, select the first AZ (e.g., *us-west-1a*). In the **CIDR block** box, type **10.200.10.0/24**
2.3.4	Click **Yes, Create**. You should be able to see **Public Subnet 1** listed in the table.
2.3.5	Repeat the steps to create another subnet with the following configuration: • In the **Name tag** box, type **Private Subnet 1** • For **VPC**, click **Lab VPC** (10.200.0.0|Lab VPC). • For **Availability Zone**, select the same AZ as for **Public Subnet 1**, which was the first AZ listed (e.g., *us-west-1a*). In the **CIDR block** box, type **10.200.50.0/24**
2.3.6	Click **Yes, Create**.

© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.

PRINTED BY: gleung@datapipe.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Configuring Route Tables

Introduction

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 2.4: Configure a route table

To create a route table that allows incoming and outgoing traffic through the Internet gateway you created earlier:

Step	Action
2.4.1	In the navigation pane, click **Route Tables**.
2.4.2	Click **Create Route Table**.
2.4.3	In the **Create Route Table** dialog box: • In the **Name tag** box, type **Public Route** • For **VPC**, click **Lab VPC**.
2.4.4	Click **Yes, Create**.
2.4.5	Select the **Public Route** you just created, and then click the **Routes** tab in the lower pane of the console.
2.4.6	Click **Edit**.
2.4.7	In the **Destination** box, type **0.0.0.0/0** For **Target**, select the **Lab VPC Gateway** that you created earlier (the ID starts with *igw-*).
2.4.8	Click **Save**.

© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.

PRINTED BY: gleung@datapipe.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Configuring Route Tables, Continued

Task 2.5: Associate the route table with subnets

To associate your public subnet with a route table to allow incoming and outgoing data flow:

Step	Action
2.5.1	With **Public Route** selected, click the **Subnet Associations** tab.
2.5.2	Click **Edit**.
2.5.3	Select the check box for **Public Subnet 1** (CIDR range of 10.200.10.0/24).
2.5.4	Click **Save**. You should now be able to see only the private subnets in a table labeled "**The following subnets have not been associated with any route tables and are therefore using the main table routes.**"
2.5.5	Click **Create Route Table**.
2.5.6	In the **Create Route Table** dialog box: • In the **Name tag** box, type **Private Route** • For **VPC**, click **Lab VPC**.
2.5.7	Click **Yes, Create**.
2.5.8	With **Private Route** selected, click the **Subnet Associations** tab if it is not already selected. **Note:** Your **Private Subnet 1** is currently associated with the **Main** route table by default.
2.5.9	Click **Edit**.
2.5.10	Select the check box for **Private Subnet 1** (CIDR range of 10.200.50.0/24).
2.5.11	Click **Save**.

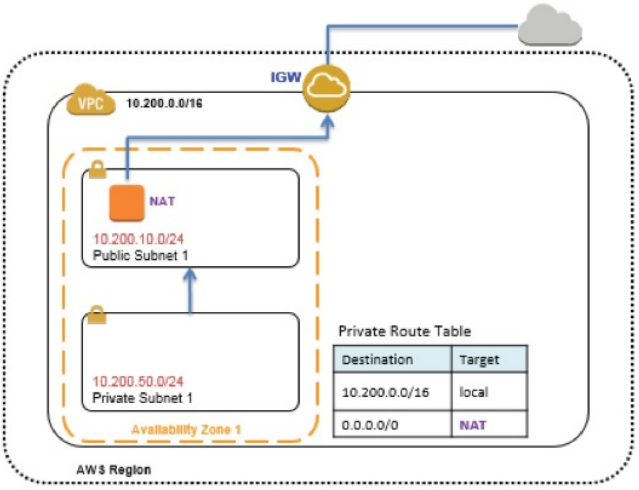
© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.

PRINTED BY: gleung@datapipe.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Creating a NAT Instance

Introduction

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.



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 2.6: Create a NAT instance

To create a NAT instance in Public Subnet 1:

Step	Action
2.6.1	On the **Services** menu, click **EC2**.
2.6.2	Click **Launch Instance**.

Continued on next page

© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.

PRINTED BY: gleung@datapipe.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Creating a NAT Instance, Continued

Task 2.6: Create a NAT instance, continued

Step	Action
2.6.3	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**.
2.6.4	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**.
2.6.5	On the **Configure Instance Details** page, make these selections: • For **Network**, select **Lab VPC**. • For **Subnet**, select **Public Subnet 1** (10.200.10.0/24). • For **Auto-assign Public IP**, select **Enable**.

Continued on next page

© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.

PRINTED BY: gleung@datapipe.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Creating a NAT Instance, Continued, Continued

Task 2.6: Create a NAT instance, continued

Step	Action

2.6.6	Expand the **Advanced Details** section. 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** field.
	
	`#!/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.

2.6.7	Click **Next: Add Storage**.
2.6.8	Accept the default, and click **Next: Tag Instance**.
2.6.9	In the **Value** box, type **NAT**
2.6.10	Click **Next: Configure Security Group**.
2.6.11	The **Create a new security group** option should be selected for **Assign a security group**. • In the **Security group name** box, type **NAT-SG** • In the **Description** box, type **NAT Security Group**

Continued on next page

© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.