



Amazon Web Services

Hands on Labs for Architecting with AWS for Partners
VPC

June 2013

Table of Contents

EC2 and VPC.....	3
Create the VPC	3
Start Your QwikLab	3
Open the AWS management Console.....	3
Launch a Stack with CloudFormation.....	5
View the CloudFormation Outputs	6
Try to Access Wordpress.....	6
Explore Your VPC.....	6
Explore your Subnets	6
Launch a Windows Instance into the Public Subnet.....	7
Open the EC2 Management Console.....	7
Explore Your Existing Instances.....	7
Launch a New Instance	8
Attach an Elastic IP Address to Your Windows Instance	8
Retrieve your Windows password	9
Remote Desktop to Your Instance	9
Building a Custom AMI.....	9
Change the Administrator Password	10
Add a Wordpress Shortcut.....	10
Create a New AMI	10
Launch an Instance from Your New AMI	10
Terminate Resources	11
Terminate Your Windows Instances	11
Delete Your CloudFormation Stack.....	11

EC2 and VPC

The objective of this exercise is to demonstrate several features of EC2 and VPC. You will begin by using CloudFormation to create a VPC with two subnets. One subnet is public (i.e., it has a route to an Internet Gateway) and contains an EC2 instance providing NAT; the other subnet is private and contains an EC2 instance that has been dynamically configured to install Wordpress and MySQL.

Because the Wordpress site is installed on a private subnet, there is no way to access it directly from the public Internet. Your objective is to access the Wordpress site, finish the installation, and write a blog post for your internal employees. Along the way you will learn about the concept of a Jump Host, Elastic IP addresses, VPC Route Tables, and Amazon Machine Images.

Create the VPC

Start Your QwikLab

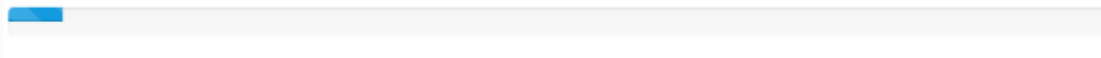
Here's how to get started with your qwikLAB™.

1. Click **Start Lab** to start your lab.
(If you are prompted for a token, please use one you've been given or have purchased.)



A progress bar appears, indicating that qwikLAB™ is preparing your lab environment.

 *Create in progress...*



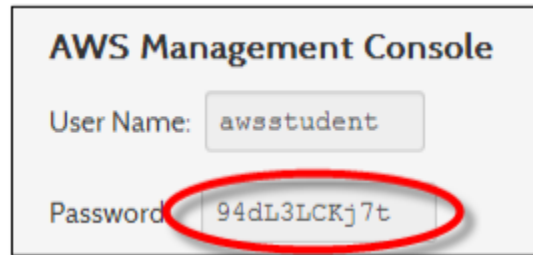
2. After your lab is ready, be sure to note:
 - a. **Duration** - The time the lab will run for before shutting itself down.
 - b. **Setup Time** - The estimated lab creation time on starting the lab.
 - c. **AWS Region** - The AWS Region the lab resources are being created in.

Open the AWS management Console

Next, you need to open the AWS Management Console.

1. Copy the Password for the AWS Management Console provided by qwikLAB™ for your lab

We recommend selecting the value shown and using Ctrl (or Command) + C. The screenshot below is an example use whatever is displayed to you

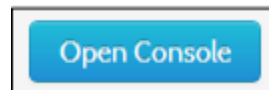


AWS Management Console

User Name:

Password:

2. Click **Open Console**.



3. Login to the AWS Management Console.
 4. Type the User Name '**awsstudent**' and paste the password you copied from the lab details in qwikLAB™ into the **Password** text box.
 5. Click Sign in using our secure server.
- You've now logged into the AWS Management Console using credentials provisioned via AWS Identity Access Management in an AWS account by qwikLAB™



Amazon Web Services Sign In

Please enter the AWS Identity & Access Management (IAM) User name and password assigned by your system administrator to sign in.

AWS Account: 832809622232

User Name:

Password:

[Sign in using our secure server](#)

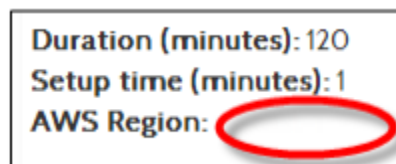
Please contact your system administrator if you have forgotten your user credentials.

[Sign in using AWS Account credentials](#)

Confirm your AWS Region

Some labs require a specific region to function correctly. Here's how to check the region for your lab.

1. Note the AWS Region set for your lab in qwikLAB™.

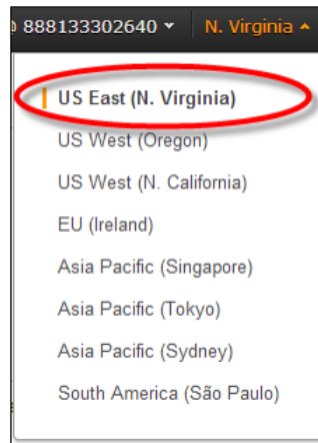


Duration (minutes): 120

Setup time (minutes): 1

AWS Region:

2. Select or confirm that the same AWS Region is already set in the AWS Management Console.



Launch a Stack with CloudFormation

To get started, you'll launch a template using a CloudFormation stack. This stack creates the a VPC with the associated resources deployed into it.

1. Download the CloudFormation template from : https://awsu-arch.s3.amazonaws.com/aux/technical-exercises/vpc/private-wordpress-via-rdp_student.template
 2. From the Services menu in the Management Console, select CloudFormation.
 3. Click Create New Stack.
 4. Select the Upload Template File option.
 5. In the Name text box, type a name for the stack.
 6. Click Choose File and select the template you downloaded, then click Continue.
 7. In the KeyName text box, type the name of the KeyPair you created. You do not need to add the extension.
 8. Check I acknowledge that this template may create IAM resources and click Continue.
 9. Click Continue again.
 10. A final confirmation screen appears. Click Continue to launch the stack.
- After a few minutes, the stack will be ready.

1. **You should now see a stack named `vpc-Exercise` with a status of `CREATE-IN-PROGRESS`**
2. Periodically refresh the screen until the 'VPC-Exercise' stack goes to `CREATE-COMPLETE`

View the CloudFormation Outputs

After your stack reaches *CREATE-COMPLETE* status, you can view some of the outputs generated by the stack. For this example, CloudFormation will output the following items:

- PublicSubnetId: The ID of the public VPC subnet created by CloudFormation
- PrivateSubnetId: The ID of the private VPC subnet created by CloudFormation
- WordpressUrl: The URL of the Wordpress instance launched into the private VPC subnet

To view these values for your CloudFormation stack, click your VPC-Exercise stack, then choose the Outputs tab in the bottom panel.

Note: IMPORTANT: copy/paste all of these output values; we'll need them throughout the exercise.

Try to Access Wordpress

Paste the WordpressUrl output value into a browser and try to access the site you launched. Why doesn't this work? How can we successfully access the Wordpress site?

Explore Your VPC

Now that you've used CloudFormation to launch a VPC, let's take a few minutes to explore it.

Open the VPC Management Console

Access the VPC management Console

Click the Your VPCs link in the left column to view information about the VPC you created in the previous step.

Explore your Subnets

Let's look at the subnets created in this VPC and observe the differences between a public and private subnet.

1. Click the Subnets tab in the left column to view the subnets created in your VPC.
2. Locate the PublicSubnetId value you copied from your CloudFormation output in the previous exercise
3. Paste that ID in the search box above the list of subnets.
4. Click the resulting public subnet item in the list and drag the bottom panel up to expand the detail view

The subnet detail view contains all of the information about the selected subnet, including its Availability Zone, associated Network ACLs, and Route Table.

Which entry in the public subnet's Route Table actually makes it public?

Repeat the previous steps, this time searching for the PrivateSubnetId

Note the differences in the private subnet's Route Table. Toggle back and forth between subnets if necessary to identify the difference.

Launch a Windows Instance into the Public Subnet

The Wordpress instance you launched in the first exercise is in a private subnet; it has a private IP address and can't be accessed from the public Internet. In this exercise, you will launch a new instance in the public subnet, and then use that instance to access Wordpress.

Open the EC2 Management Console

Access the EC2 Console

Explore Your Existing Instances

Before launching a new instance, let's look at the existing EC2 instances you created in the first exercise.

1. Click the Instances link in the left column
2. You should have two running instances, one named NAT Instance and the other Wordpress. **The NAT Instance is an EC2 instance running in the public subnet. When properly configured, NAT provides other EC2 instances in a private subnet the ability to initiate outbound connections to the public Internet, but does not allow inbound connections to be initiated from the Internet (i.e., instances in a private subnet still only have a private, non-routable IP address). This is useful, for example, when you have instances in a private subnet, but want them to be able to download OS updates. In this example, we needed the NAT instance to allow the private instance to download the Wordpress software from the Internet.**
3. Select one of the instances and observe the detail panel. Look for the Subnet ID of the instance to determine which subnet it is running in. **Refer back to the output of your CloudFormation stack to match the subnet ID with the public and private values.**

Launch a New Instance

Now you will launch a new EC2 instance running Windows Server 2008 R2 into the public subnet. After launching the instance, you will retrieve its password and make a RDP connection to it

1. Click the above your list of instances
2. Click
3. Locate the Microsoft Windows Server 2008 R2 Base AMI in the list and click
4. Change Instance Type to m1.medium **This step is important. The default value for Instance Type is t1.micro, but that type is not currently supported in VPC.**
5. For the Launch Into option, choose VPC and select the public subnet in the Subnet dropdown **Refer back to the output of your CloudFormation stack to locate the ID of your public subnet**
6. Click
7. Click again
8. Give your instance a name (e.g., Windows Server) and click
9. Choose your Key Pair and click
10. Click Create a new Security Group
 - a. Enter *RDP* for the Group Name and Group Description
 - b. Choose *RDP* from the dropdown
 - c. Click Add Rule, then click
 - d. Click

Creating the Security Group in this fashion allows inbound connections from the Internet to TCP port 3389 (i.e., Remote Desktop Protocol) for EC2 instances launched into the Security Group.

Attach an Elastic IP Address to Your Windows Instance

Even though you've launched this instance into the public subnet, it still only has a private IP address that is not addressable from the public Internet. When the state of your new instance changes to running (with a green dot), provision a new public Elastic IP and attach it to the instance.

1. Click the Elastic IPs link in the left column
2. Click Allocate New Address near the top of the screen
3. Choose VPC from the dropdown

4. Click Yes, Allocate

Now that we've provisioned a new IP, you can attach it to your Windows Instance.

5. Select the Elastic IP in the list, then click the Associate Address button
6. In the Instance list, find the name you assigned to the Windows instance launched previously
7. Click Yes, Associate One of the unique, valuable characteristics of Elastic IP addresses is their ability to be detached from one EC2 Instance and attached to another.
8. Copy and paste the Elastic IP address somewhere accessible

Your Windows instance now has a public Elastic IP address. We'll use this in the next step to access your Windows instance via Remote Desktop. But first you will need to decrypt your Windows password.

Retrieve your Windows password

1. Access the Instances section from the EC2 Console
2. Right-click your Windows instance and choose Get Windows Password
3. In the Private Key field, click Choose File and locate the `.pem` for the Key Pair you launched the instance with
4. Click Decrypt Password
5. Paste the decrypted password alongside the Elastic IP address from the previous section

Remote Desktop to Your Instance

1. Using the Administrator user name and the password and IP address pasted above, use Remote Desktop to login to your Windows instance.
2. Once you're at the desktop, open Internet Explorer and paste the WordpressUrl (from the output of your CloudFormation stack in the first exercise). Follow the steps to complete the Wordpress setup and write your first blog post. Note you may wish to disable the I.E

Congratulations! You successfully used VPC to isolate an application in a private subnet and access it from the public subnet.

Building a Custom AMI

EC2 makes it very simple to customize a running instance and bundle your changes into a private AMI that you can use to launch new instances. In this exercise, you will make a modification to your Windows instance, create a new AMI based on your changes, and launch a new instance from your custom AMI.

Change the Administrator Password

1. Click Start > Windows Security and choose Change a Password
2. Provide the old password as well as a new password

Note: the new password should be somewhat complex to meet strong default password policy requirements

Add a Wordpress Shortcut

Right-click the desktop and choose **New > Shortcut**. Paste the Wordpress URL, click Next and give the shortcut a name.

Create a New AMI

1. Find your Windows instance in the EC2 Console
2. Right-click the instance and choose Create Image (EBS AMI)
3. Give the image a name and description, then click Create This Image.

Note: The running instance will be stopped while the AMI is created. Any existing RDP session will be closed.

Launch an Instance from Your New AMI

Follow the steps below to launch a new instance from the AMI you just created

1. Click the AMIs link in the left column to view your AMIs
2. Wait for your new AMI's status to change to available
3. Right-click the AMI and choose Launch Instance
4. Using skills from the previous section, choose the correct instance type, subnet, key pair, security group, etc. to launch the new instance such that it is in the public subnet and you can Remote Desktop to it
5. After the instance is launched and available, allocate a new Elastic IP address and attach it to the new instance.
6. Use Remote Desktop to access the new instance at the IP address created in the previous step. **Remember, your password change was incorporated into the AMI you used to launch this instance.**
7. Confirm that your Wordpress shortcut is available and functioning

Congratulations! You successfully customized a running instance and created a new AMI to capture those changes. You can use the new AMI to launch different instances of different sizes into various locations.

Click through to the next section as it's very important (instructions for terminating all resources created in this exercise)

Terminate Resources

All of the resources created in this exercise will contribute to your monthly bill. It's important to follow each of the below steps to terminate all of the resources so you aren't charged beyond the short duration of this exercise.

In addition to completing all of the below steps, it is important that you complete them *in order*.

Terminate Your Windows Instances

Locate the two Windows instances you manually launched in the EC2 Management Console.

1. Right-click each instance, then choose Terminate

Note: IMPORTANT: Check the Release Elastic IPs checkbox

2. Click Yes, Terminate
3. Perform these steps for each of the two Windows instances you launched

Delete Your CloudFormation Stack

1. Locate the VPC-Exercise stack in the CloudFormation Management Console.
2. Select the stack, then click Delete Stack
3. Click Yes, Delete

Note: Because you used CloudFormation to provision the VPC and Wordpress instance, it will take care of removing all of those resources