EXERCISE 3.1

Launch and Connect to a Linux Instance

In this exercise, you will launch a new Linux instance, log in with SSH, and install any security updates.

1. Launch an instance in the Amazon EC2 console.

2. Choose the Amazon Linux AMI.

3. Choose the **t2.micro** instance type.

4. Launch the instance in the **default VPC**.

5. Assign the instance a public IP address.

6. Add a tag to the instance of **Key: Name, Value: Exercise 3.1.**

7. Create a new security group called **Exercise_SG**.

8. Add a rule to **Exercise** allowing SSH access from the IP address of your workstation.

9. Launch the instance.

10. When prompted for a key pair, choose a key pair you already have or create a new one and download the private portion.

Amazon generates a keyname.pem file, and you will need a keyname.ppk file to connect to the instance via SSH. Puttygen.exe is one utility that will create a .ppk file from a .pem file.

11. SSH into the instance using the public IP address, the user name ec2-user, and the keyname.ppk file.

12. From the command-line prompt, run **sudo yum update -y**.

13. Close the SSH window and terminate the instance.

EXERCISE 3.2

Launch a Windows Instance with Bootstrapping

In this exercise, you will launch a Windows instance and specify a very simple bootstrap script. You will then confirm that the bootstrap script was executed on the instance.

1. Launch an instance in the Amazon EC2 console.
2. Choose the Microsoft Windows Server 2012 Base AMI.
3. Choose the t2.micro instance type.
4. Launch the instance in either the default VPC.
5. Assign the instance a public IP address.
6. In the Advanced Details section, enter the following text as UserData:
   <script>
   md c:\temp
   </script>

7. Add a tag to the instance of Key: Name, Value: Exercise 3.2.
8. Use the **Exercise_SG** security group from Exercise 3.1.
9. Launch the instance.
10. Use the key pair from Exercise 3.1.
11. On the Connect Instance UI, decrypt the administrator password and then download the RDP file to attempt to connect to the instance. Your attempt should fail because the **Exercise_SG** security group does not allow RDP access.
12. Open the **Exercise_SG** security group and add a rule that allows RDP access from your IP address.
13. Attempt to access the instance via RDP again.
14. Once the RDP session is connected, open Windows Explorer and confirm that the
15. c:\temp folder has been created.
16. End the RDP session and terminate the instance

EXERCISE 3.3

Access Metadata. In this exercise, you will access the instance metadata from the OS.

1. Launch an instance in the Amazon EC2 console.

2. Choose the Amazon Linux AMI.

3. Choose the t2.micro instance type.

4. Launch the instance in either the default VPC.

5. Assign the instance a public IP address.

6. Add a tag to the instance of Key: Name, Value: Exercise 3.5.

7. Use the **Exercise_SG** security group.

8. Launch the instance.

9. Use the key pair from Exercise 3.1.

10. Connect the instance via SSH using the public IP address, the user name ec2-user, and the keyname.ppk file.

11. At the Linux command prompt, retrieve a list of the available metadata by typing: curl http://169.254.169.254/latest/meta-data/

12. To see a value, add the name to the end of the URL. For example, to see the security groups, type: curl http://169.254.169.254/latest/meta-data/security-groups

13. Try other values as well. Names that end with a / indicate a longer list of sub-values.

14. Close the SSH window and terminate the instance

EXERCISE 3.4

Create an Amazon EBS Volume and Show That It Remains After the Instance Is Terminated. In this exercise, you will see how an Amazon EBS volume persists beyond the life of an instance.

1. Launch an instance in the Amazon EC2 console.

2. Choose the Amazon Linux AMI.

3. Choose the t2.micro instance type.

4. Launch the instance in the default VPC.

5. Assign the instance a public IP address.

6. Add a second Amazon EBS volume of size 5 GB. **Note that the Root Volume is set to delete on Termination.**

7. Add a tag to the instance of Key: Name, Value: Exercise 3.4.

8. Use the **Exercise_SG** security group from earlier exercises.

9. Launch the instance.

10. Find the two Amazon EBS volumes on the Amazon EBS console. Name them both Exercise 3.4.

11. Terminate the instance.

Notice that the boot drive is destroyed, but the additional Amazon EBS volume remains and now says Available. Do not delete the Available volume.

EXERCISE 3.5

Take a Snapshot and Restore. This exercise guides you through taking a snapshot and restoring it in three different ways.

1. Find the volume you created in Exercise 3.4 in the Amazon EBS console.

2. Take a snapshot of that volume. Name the snapshot Exercise 3.5.

3. On the snapshot console, wait for the snapshot to be completed.

4. On the snapshot page in the AWS Management Console, choose the new snapshot and select Create Volume.

5. Create the volume with all the defaults.

6. Locate the snapshot again and again choose Create Volume, setting the size of the new volume to 10 GB (taking a snapshot and restoring the snapshot to a new, larger volume is how you address the problem of increasing the size of an existing volume).

9. Delete all volumes.

EXERCISE 3.6

Detach a Boot Drive and Reattach to another Instance. In this exercise, you will practice removing an Amazon EBS volume from a stopped drive and attaching to another instance to recover the data.

1. Launch an instance in the Amazon EC2 console.

2. Choose the Microsoft Windows Server 2012 Base AMI.

3. Choose the t2.micro instance type.

4. Launch the instance in the default VPC.

5. Assign the instance a public IP address.

6. Add a tag to the instance of Key: Name, Value: Exercise 3.6 Source.

7. Use the **Exercise_SG** security group from earlier exercises.

8. Launch the instance with the key pair from Exercise 3.1.

9. Launch a second instance in the Amazon EC2 Console.

10. Choose the Microsoft Windows Server 2012 Base AMI.

11. Choose the t2.micro instance type.

12. Launch the instance in the default VPC.

13. Assign the instance a public IP address.

14. Add a tag to the instance of Key: Name, Value: Exercise 3.9 Destination.

15. Use the **Exercise_SG** security group from earlier exercises.

16. Launch the instance with the key pair you used in Exercise 3.1.

17. Once both instances are running, stop the first instance (Source). Make a note of the instance ID.

18. Go to the Amazon EBS page in the Amazon EC2 console and find the volume attached to the Source instance via the instance ID. Detach the instance.

19. When the volume becomes Available, attach the instance to the second instance

(Destination).

20. Log in to the Destination instance via RDP using the administrator account.

21. Open a command window (cmd.exe).

22. At the command prompt, type the following commands:

```
C:\Users\Administrator >diskpart

DISKPART>select disk 1
```

DISKPART>online disk

DISKPART>exit

C:\Users\Administrator>dir e:

The volume removed from the stopped source drive can now be read as the E: drive on the destination instance, so its data can be retrieved.

23. Terminate all the instances and ensure the volumes are deleted in the process.

EXERCISE 3.6

Create an Elastic Load Balancing Load Balancer

In this exercise, you will use the AWS Management Console to create an Elastic Load Balancing load balancer.

1. Launch an Amazon EC2 instance using an AMI with a web server on it, or install and configure a web server.

2. Create a static page to display and a health check page. Configure the Amazon EC2 instance to accept traffic over port 80.

3. Register the Amazon EC2 instance with the Elastic Load Balancing load balancer, and configure it to use the health check page to evaluate the health of the instance.

EXERCISE 3.7

Use an Amazon CloudWatch Metric

1. Launch an Amazon EC2 instance.

2. Use an existing Amazon CloudWatch metric to monitor a value.

EXERCISE 3.8

Create a Scaling Policy

1. Create an Amazon Cloud Watch metric and alarm for CPU utilization using the AWS Management Console.

2. using the Auto Scaling group from Exercise 5.4, edit the Auto Scaling group to include a policy that uses the CPU utilization alarm.

3. Drive CPU utilization on the monitored Amazon EC2 instance(s) up to observe Auto Scaling.

EXERCISE 3.9

Create a Web Application That Scales

1. Create a small web application architected with an Elastic Load Balancing load balancer, an Auto Scaling group spanning two Availability Zones that uses an Amazon CloudWatch metric, and an alarm attached to a scaling policy used by the Auto Scaling group.

2. Verify that Auto Scaling is operating correctly by removing instances and driving the metric up and down to force Auto Scaling.