Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Elastic Block Store (Amazon EBS)

EXERCISE - 2.1

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.medium instance type.
4. Launch the instance in either the default VPC or EC2-Classic.
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 **`Cert Book`**.
8. Add a rule to Cert Book allowing SSH access from the IP address of your workstation (`www.WhatsMyIP.org` is a good way to determine your IP address).
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—security -y`.
13. Close the SSH window and terminate the instance.

EXERCISE - 2.2

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.medium instance type.
4. Launch the instance in either the default VPC or EC2-Classic.
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 Cert Book 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 Cert Book security group does not allow RDP access.
12. Open the Cert Book 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 `c:\temp` folder has been created.
15. End the RDP session and terminate the instance.

EXERCISE - 2.3

Confirm That Instance Stores Are Lost When an Instance Is Stopped

In this exercise, you will observe that the data on an Amazon EC2 instance store is lost when the instance is stopped.

1. Launch an instance in the Amazon Management Console.
2. Choose the Microsoft Windows Server 2012 Base AMI.
3. Choose the m3.medium instance type.
4. Launch the instance in either the default VPC or EC2-Classic.
5. Assign the instance a public IP address.
6. Add a tag to the instance of Key: Name, Value: **`Exercise 3.3`**.
7. Use the Cert Book security group as updated in Exercise 3.2.
8. Launch the instance.
9. Use the key pair from Exercise 3.1.

10. Decrypt the administrator password login to the instance via RDP.
11. Once the RDP session is connected, open Windows Explorer.
12. Create a new folder named `z:\temp`.
13. Log out of the RDP session.
14. In the console, set the state of the instance to Stopped.
15. Once the instance is stopped, start it again.
16. Log back into the instance using RDP.
17. Open Windows Explorer and confirm that the `z:\temp` folder is gone.
18. End the RDP session and terminate the instance.

EXERCISE - 2.4

Launch a Spot Instance

In this exercise, you will create a Spot Instance.

1. In the Amazon EC2 console, go to the Spot Request page.
2. Look at the pricing history for m3.medium, especially the recent price.
3. Make a note of the most recent price and Availability Zone.
4. Launch an instance in the Amazon EC2 console.
5. Choose the Amazon Linux AMI.
6. Choose the t2.medium instance type.
7. On the Configure Instance page, request a Spot Instance.
8. Launch the instance in either the Default VPC or EC2-Classic. (Note the Default VPC will define the Availability Zone for the instance.)
9. Assign the instance a public IP address.
10. Request a Spot Instance and enter a bid a few cents above the recorded Spot price.
11. Finish launching the instance.
12. Go back to the Spot Request page.

    Watch your request. If your bid was high enough, you should see it change to Active and an instance ID appear.

13. Find the instance on the instances page of the Amazon EC2 console. Note the Lifecycle field in the Description that says Spot.
14. Once the instance is running, terminate it.

EXERCISE - 2.5

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.medium instance type.
4. Launch the instance in either the default VPC or EC2-Classic.
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 Cert Book 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 - 2.6

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.medium instance type.
4. Launch the instance in either the default VPC or EC2-Classic.
5. Assign the instance a public IP address.
6. Add a second Amazon EBS volume of size 50 GB. Note that the Root

Volume is set to Delete on Termination.

7. Add a tag to the instance of Key: Name, Value: `Exercise 3.6`.
8. Use the Cert Book 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 3.6`.
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 - 2.7

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 3.6 in the Amazon EBS console.
2. Take a snapshot of that volume. Name the snapshot `Exercise 3.7`.
3. On the snapshot console, wait for the snapshot to be completed. (As the volume was empty, this should be very quick.)
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 100 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). Locate the snapshot again and choose Copy. Copy the snapshot to another region. Make the description `Exercise 3.7`.
7. Go to the other region and wait for the snapshot to become available.
8. Create a volume from the snapshot in the new region. This is how you share an Amazon EBS volume between regions; that is, by taking a snapshot and copying the snapshot.
9. Delete all four volumes.

EXERCISE - 2.8

Launch an Encrypted Volume

In this exercise, you will launch an Amazon EC2 instance with an encrypted

Amazon EBS volume and store some data on it to confirm that the encryption is transparent to the instance itself.

1. Launch an instance in the Amazon EC2 console.
2. Choose the Microsoft Windows Server 2012 Base AMI.
3. Choose the m3.medium instance type.
4. Launch the instance in either the default VPC or EC2-Classic.
5. Assign the instance a public IP address.
6. On the storage page, add a 50 GB encrypted Amazon EBS volume.
7. Add a tag to the instance of Key: Name, Value: **`Exercise 3.8`**.
8. Use the Cert Book security group as updated in Exercise 3.2.
9. Launch the instance.
10. Choose the key pair from Exercise 3.1.
11. Decrypt the administrator password and log in to the instance using RDP.
12. Once the RDP session is connected, open Notepad.
13. Type some random information into Notepad, save it at `d:\testfile.txt`, and then close Notepad.
14. Find `d:\testfile.txt` in Windows Explorer and open it with Notepad. Confirm that the data is not encrypted in Notepad.
15. Log out.
16. Terminate the instance.

EXERCISE - 2.9

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.medium instance type.
4. Launch the instance in either the default VPC or EC2-Classic.
5. Assign the instance a public IP address.
6. Add a tag to the instance of Key: Name, Value: **`Exercise 3.9 Source`**.
7. Use the Cert Book 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.medium instance type.
12. Launch the instance in either the default VPC or EC2-Classic.
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 Cert Book 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.