

Ec2- assignment 2 submitted by kalaiselvan

1. How will you recover your data in EC2 if you lost your key pair?
2. How to upgrade the instance in aws?
3. How will connect From One EC2(Linux) to another EC2(linux)?
4. How will you copy the data from one ec2(linux) to another ec2(linux)?
5. Install httpd using user data in EC2 instance?
6. How many inbound & Outbound rules we can configure in Security Group?
7. How many Inbound & Outbound rules we can able to configure in NACL?
8. is it possible to restrict a user in Security Group?
9. How will you restrict a user in NACL?
10. How will migrate the EBS Volume from one zone to another zone?

1. How will you recover your data in EC2 if you lost your key pair?

Method 1: creating AMI from the original instance and launch a new instance from the ami:

If you have access to the instance, you can create an AMI (Amazon Machine Image) of the instance. This will create a snapshot of the instance, including the data stored on the instance. You can then launch a new instance from the AMI, and you will be able to access the data from the original instance.

Method2: detach the root volume from the original instance and attach it to a recovery instance and access it

Method3: Recover access to your EC2 Instance after losing your key-pair

<https://medium.com/the-10x-dev/how-to-recover-access-login-to-your-aws-instance-after-losing-your-pem-keypair-file-e0d31bae2da4>

the steps required and covered in this post to recover access to your EC2 Instance after losing your key-pair

- *Gather config details of the original(target) instance.*
- *Power off the original(target) EC2 instance of which you want to regain access.*
- *Launch new (recovery) instance and generate new key-pair*
- *Login via ssh to the new recovery instance*
- *Detach the primary EBS volume from original(target) instance (taking note of its current attachment)*
- *Attach/Mount the previously detached volume to the new(recovery) instance*
sudo mkdir /mnt/tempvol #this creates a temporary mount directory.
sudo mount /dev/xvdf1 /mnt/tempvol #this mounts the volume on the temporary mount directory.
- *Copy authorized keys from recovery instance to the mounted (target) volume*

- *Unmount target volume from recovery instance and reattach back to original (target) instance using configs noted earlier*
- *Start the original (target) instance and login with new key-pair*
- *Delete temporary(recovery) instance*

(useful commands:

`df -h`

command is used to display the free disk space on all mounted filesystems on your system.

The -h option tells the command to display the sizes in human-readable format, which is more convenient to understand than the raw bytes.

`lsblk -f` -to view all blocks attached to the instance

`sudo mkdir /mnt/tempvol` - this creates a temporary mount directory

`sudo mount /dev/xvda /mnt/tempvolume` #this mounts the volume on the temporary mount directory

`lsblk -f` #now you will see the new volume mounted at /mnt/tempvol)

`lsblk -f` #now you will see the new volume mounted at /mnt/tempvol)

(<https://www.youtube.com/watch?v=IbaYMFyH89E>)

2. How to upgrade the instance in aws?

The steps on how to upgrade an instance in AWS:

Check the compatibility of your instance type. Not all instance types are compatible with each other. You can check the compatibility of your instance type in the AWS documentation.

Back up your data. Before you upgrade your instance, it is important to back up your data.

This is because there is a risk of data loss during the upgrade process.

Stop your instance. You cannot upgrade an instance that is running. So, you need to stop your instance before you can upgrade it.

Change the instance type. In the AWS console, go to the EC2 dashboard and select the instance that you want to upgrade. Then, click on the "Change Instance Type" button.

Select the new instance type. In the "Change Instance Type" dialog box, select the new instance type that you want to use. Then, click on the "Change" button.

Start your instance. Once the instance type has been changed, you can start your instance again.

Here are some additional things to keep in mind when upgrading an instance in AWS:

- For upgrading a Windows instance, you may need to install the drivers for the new instance type.
- For upgrading an instance that is running a specific application, you may need to make some changes to the application configuration.

The changes can be:

Updating the application's memory requirements. The new instance type may have a different amount of memory than the old instance type. So, you may need to update the application's memory requirements in the configuration file.

Updating the application's CPU requirements. The new instance type may have a different amount of CPU than the old instance type. So, you may need to update the application's CPU requirements in the configuration file.

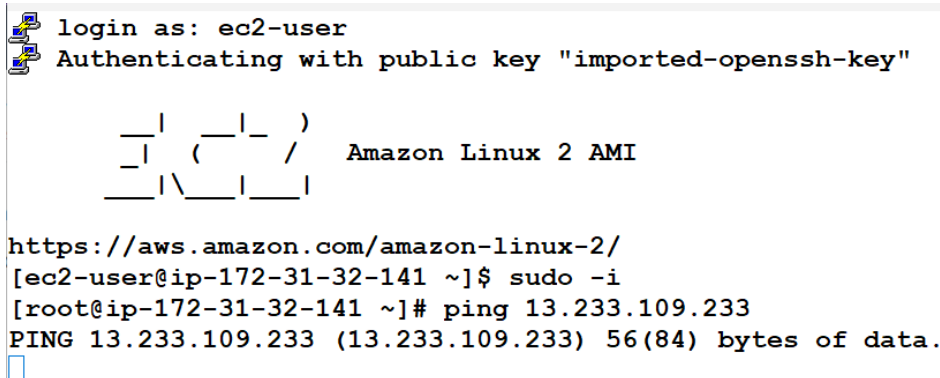
Updating the application's network settings. The new instance type may have a different network configuration than the old instance type. So, you may need to update the application's network settings in the configuration file.

Updating the application's database settings. If the application uses a database, you may need to update the database settings in the configuration file.

3. How to connect One EC2(Linux) to another EC2(linux)?

Steps:

- 1) Go to EC2 console and note down IP and security ID of both the linux instances
Linux1 --- Instance ID: i-08de0236286c8562b, SG id: sg-03795c50c3240a04d
Linux2--- Instance ID: i-0bb5ead51d2066ee4, SG id: sg-03795c50c3240a04d
- 2) Select any one instance and open network and security option
- 3) Select your instance's security group, click on inbound rules and click on edit
- 4) Now Select All ICMP-ipv4 under Type drop-down, set source tab to custom and in the next box enter the security group id of the other instance (which is "sg-d0e7d4b9") click on save button
- 5) To make the communication open from other instance as well, follow the steps 2 to 4 for other security group "sg-d0e7d4b9" and in the step 4 enter below details and click save button.
- 6) After above configuration we are now able to ping the first instance via second instance
[root@ip- 172-31-32-141 ~]# ping 13.233.109.233
PING 13.233.109.233 (13.233.109.233) 56(84) bytes of data.



```
login as: ec2-user
Authenticating with public key "imported-openssh-key"

      _|_  _|_  )
      _|_  ( _|_ /  Amazon Linux 2 AMI
      _|_  \ _|_  |

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-32-141 ~]$ sudo -i
[root@ip-172-31-32-141 ~]# ping 13.233.109.233
PING 13.233.109.233 (13.233.109.233) 56(84) bytes of data.
□
```

4. How will you copy the data from one ec2(linux) to another ec2(linux)?

Using scp command:

Login into two servers (server1&server2) using putty terminal

Create a directory (test) and file inside(test1- type some content inside) one server(server1)

List (ls -l) to see

To copy a directory from current server(server1) to destination server (server2)

scp -r A B:/ (A is source directory, B is destination server ip

scp -r /test.pem 3.109.216.51:/ (:/ (to save outside , /kalai (a directory in destination server i.e server2)))

eg1:

scp ~/Desktop/example.txt myuser@192.168.0.100:/tmp

scp ~/ C:\Users\kalai\Desktop\test.pem ec2-user@192.168.0.100:/tmp

Worked command from local command prompt to linux aws server

scp -r C:\Users\kalai\Desktop\test.pem ec2-user@3.109.216.51

```
C:\Users\kalai>scp -r C:\Users\kalai\Desktop\test.pem ec2-user@3.109.216.51
1 file(s) copied.

C:\Users\kalai>
```

5. Install httpd using user data in EC2 instance?

To launch a server with httpd through user data can be done by using shell script:

```
#!/bin/bash
yum update -y
yum install httpd -y
systemctl start httpd
systemctl enable httpd
```

or

```
#!/bin/bash
yum update -y
yum install httpd -y
service httpd start
service httpd enable
```

6. How many inbound & Outbound rules we can configure in Security Group?

Inbound Rules: By default, you can have up to 60 inbound rules per security group.

Outbound Rules: By default, you can have an unlimited number of outbound rules per security group.

7. How many Inbound & Outbound rules we can able to configure in NACL?

inbound Rules: By default, you can have up to 20 inbound rules per NACL.

Outbound Rules: By default, you can have up to 20 outbound rules per NACL.

8. is it possible to restrict a user in Security Group?

In summary, it is possible to restrict a user's access using a security group. Security groups act as virtual firewalls and allow you to control inbound and outbound traffic for instances or resources within a network. By configuring the rules within a security group, you can define restrictions based on criteria such as the user's IP address, port numbers, or other factors. This enables you to limit a user's access to specific resources, protocols, ports, or IP ranges, providing tighter control over their network connectivity. However, it's important to note that security groups operate at the network level and control traffic at the instance level, so the restrictions are applied to network traffic rather than individual users specifically.

9. How will you restrict a user in NACL?

To restrict a user's access using a Network Access Control List (NACL), you can configure inbound and outbound rules within the NACL. By defining these rules, you can control the flow of traffic to and from subnets or network resources. NACLs operate at the subnet level and provide an additional layer of network security. To restrict a user, you would create or modify the NACL associated with the subnet where the user's resources reside. Inbound rules can be used to allow or deny traffic based on the user's IP address, while outbound rules can control the user's outbound traffic by allowing or denying specific protocols or port ranges. It's important to consider rule priorities and order within the NACL, ensuring more specific rules take precedence over broader rules. Finally, the NACL needs to be applied to the appropriate subnet(s) to enforce the access restrictions. Remember that NACLs are stateless,

so inbound and outbound rules must be defined separately, and the restrictions will affect all users or resources within the associated subnet.

10.How will migrate the EBS Volume from one zone to another zone?

To migrate an Amazon EBS volume from one Availability Zone to another within the same region, follow these steps:

- Create a new EBS volume in the target zone.
- Attach the new volume to an EC2 instance.
- Copy the data from the source volume to the new volume.
- Verify the data on the new volume.
- Detach the source volume.
- Attach the new volume to the desired instance.
- Update relevant configurations to reference the new volume.

Take proper backups before performing any migration tasks to prevent data loss.