

Homework 3 EC2 and Firewalls

Name: **Pradeep Medagiri**

You work for a start-up company and you are asked to spin-up 3 virtual machines (EC2s). Each EC2 is for specific purpose.

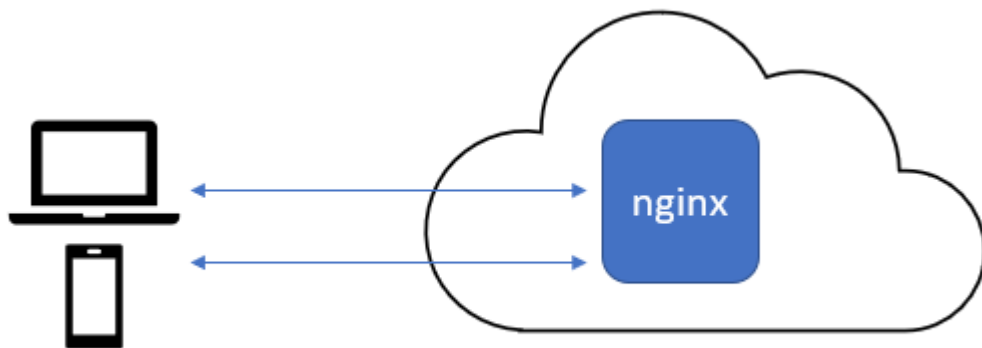
- The first machine is for a web server.
- The second is for general purpose.
- The third one is reserved for internal use only and not accessible from the outside.

At this point the company just need a simple network so you only use the AWS default VPC. Any configurations not mentioned in the problem means it is for you to decide.

All EC2 are to have:

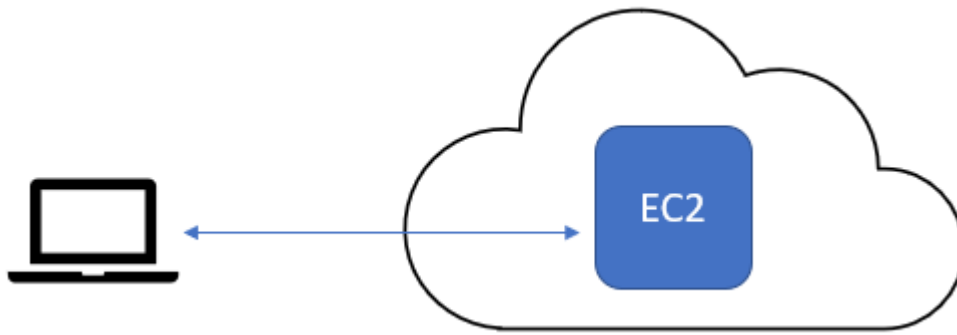
- Instance type: t2.micro.
- AMI: ubuntu.

1. First EC2 (Web Server)



- Name it your_lastname1
- Setup:
 - ssh from everywhere
 - Have a public IP
 - Allow ping from everywhere
 - Allow http call from everywhere
- Install nginx – modify so it will say in the first line: “This is ‘your-first and last name’”

2. Second EC2 (General purpose)

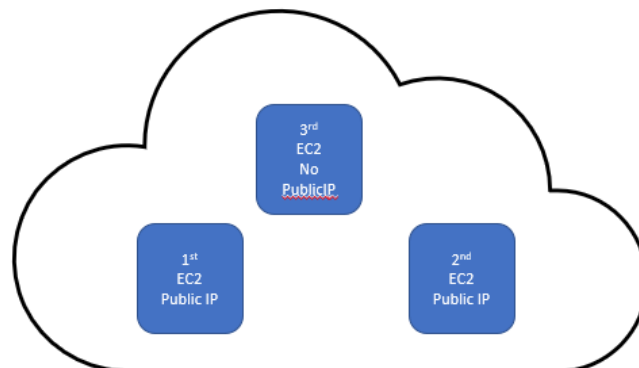


- Name it your_lastname2
- Set-up:
 - ssh from everywhere
 - has a public IP
 - there is a concerned about Ping Of Death (POD) so you want to allow ping from your laptop only

3. Third EC2 (Internal use only)

- Name it your_lastname3
- You want to reserve and protect this EC2 for special program that can not be accessed from the outside.
Setup:
 - ssh from the first EC2 only
 - No public IP
 - Allow ping from your first EC2 only

The VPC will look like this



Pradeep_Medagiri - HOMEWORK-3

Problem 1 (13):

- a) The screenshot of the 1st EC2 information, which shows: the name, Public IP address, and the Security group name (3)

For 1st EC2 – Medagiri1

Name:

The screenshot shows the AWS Management Console interface. On the left, there is a navigation menu with options like 'EC2 Dashboard', 'Events', 'Tags', 'Limits', 'Instances', 'Instance Types', 'Launch Templates', 'Spot Requests', 'Savings Plans', 'Reserved Instances', 'Dedicated Hosts', 'Scheduled Instances', 'Capacity Reservations', and 'Images'. The main content area displays the details for the EC2 instance 'Medagiri1'. The instance is in the 'running' state, located in the 'us-east-1c' availability zone. The public DNS is 'ec2-3-80-230-117.compute-1.amazonaws.com'. Below the instance details, there is a 'Tags' section with a table showing the instance's name and value.

Key	Value
Name	Medagiri1

Public IP Address:

The screenshot shows the AWS Management Console interface, similar to the previous one, but with a focus on the public IP address. The instance 'Medagiri1' is shown in the 'running' state. The public IP address is '54.242.18.83'. The security group is 'launch-wizard-1'. The instance is located in the 'us-east-1c' availability zone. The private DNS is 'ip-172-31-22-202.ec2.internal'. The private IP is '172.31.22.202'. The VPC ID is 'vpc-0de31b70'. The platform is 'Ubuntu'. The network interfaces are 'eth0'. The IAM role is 'RunInstances'. The public DNS is 'ec2-54-242-18-83.compute-1.amazonaws.com'.

Key	Value
Instance state	running
Instance type	t2.micro
Private DNS	ip-172-31-22-202.ec2.internal
Private IPs	172.31.22.202
Secondary private IPs	
VPC ID	vpc-0de31b70
Platform	Ubuntu
Platform details	Linux/UNIX
Usage operation	RunInstances
Availability zone	us-east-1c
Security groups	launch-wizard-1, view inbound rules, view outbound rules
Scheduled events	No scheduled events
AMI ID	ubuntu/images/hvm-ssd/ubuntu-bionic-18.04-amd64-server-20200903 (ami-06b263d6ceff0b3dd)
Subnet ID	subnet-d0c8b49d
Network interfaces	eth0
IAM role	RunInstances

Security group name:

The screenshot shows the AWS Management Console interface. On the left is a navigation menu with categories like Volumes, Snapshots, Lifecycle Manager, Network & Security, Load Balancing, and Auto Scaling. The main content area displays the details for a security group named 'sg-0d3d4deb83b633391 - launch-wizard-1'. At the top, there are buttons for 'Delete security group' and 'Copy to new security group'. Below this is a 'Details' section with a table of attributes:

Details			
Security group name launch-wizard-1	Security group ID sg-0d3d4deb83b633391	Description launch-wizard-1 created 2020-09-15T21:38:11.315-05:00	VPC ID vpc-0de31b70
Owner 431429019981	Inbound rules count 3 Permission entries	Outbound rules count 1 Permission entry	

Below the details table are tabs for 'Inbound rules', 'Outbound rules', and 'Tags'. The footer of the console shows 'Feedback', 'English (US)', and copyright information for Amazon Web Services, Inc.

b) The screenshot of the webpage called from your laptop (2)

For 1st - EC2:

The screenshot shows a web browser window with the address bar displaying '54.242.18.83'. The browser's file explorer shows a path: Apps > univ > extra > BA/DS/DA > decision > UTA > ML > latest > DATA Science > current. The main content of the page is a welcome message from nginx:

This is 'Pradeep Medagiri'

Welcome to nginx!

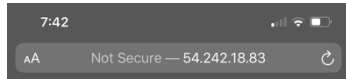
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

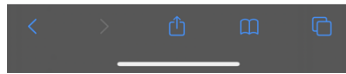
Thank you for using nginx.

c) The screenshot of the webpage called from your smartphone (2)

For 1st - EC2:



This is 'Pradeep Medagiri'
Welcome to nginx!
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.
For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.
Thank you for using nginx.

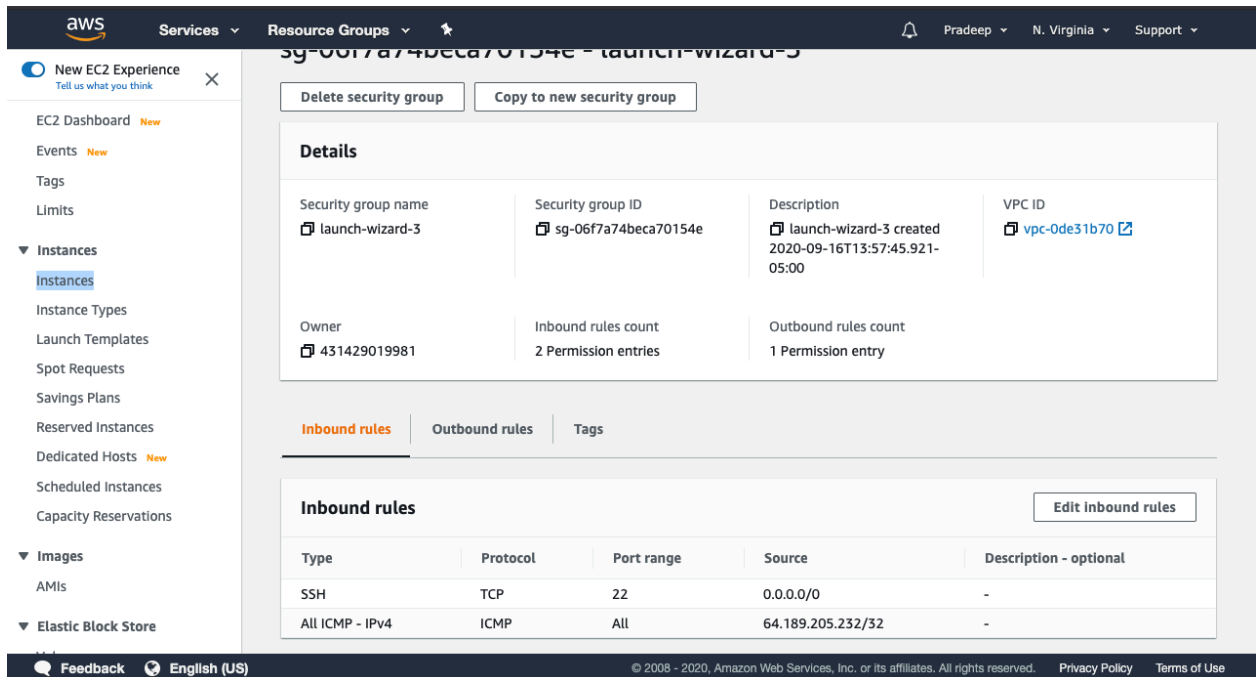


d) The screenshot of the Security group that shows the rules for incoming traffic of the 1st EC2 (2)

A screenshot of the AWS Management Console interface. The top navigation bar shows the AWS logo, 'Services', 'Resource Groups', and user information. The left sidebar contains a list of services, with 'Network & Security' expanded. The main content area shows the details of a security group named 'launch-wizard-1'. The 'Details' section includes fields for 'Security group name', 'Security group ID', 'Description', 'VPC ID', 'Owner', 'Inbound rules count', and 'Outbound rules count'. Below this, there are tabs for 'Inbound rules', 'Outbound rules', and 'Tags'. The 'Inbound rules' tab is selected, showing a table of rules. The table has columns for 'Type', 'Protocol', 'Port range', 'Source', and 'Description - optional'. There are three rules listed: HTTP (TCP, port 80, source 0.0.0.0/0), SSH (TCP, port 22, source 0.0.0.0/0), and All ICMP - IPv4 (ICMP, port All, source 0.0.0.0/0).

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	0.0.0.0/0	-
SSH	TCP	22	0.0.0.0/0	-
All ICMP - IPv4	ICMP	All	0.0.0.0/0	-

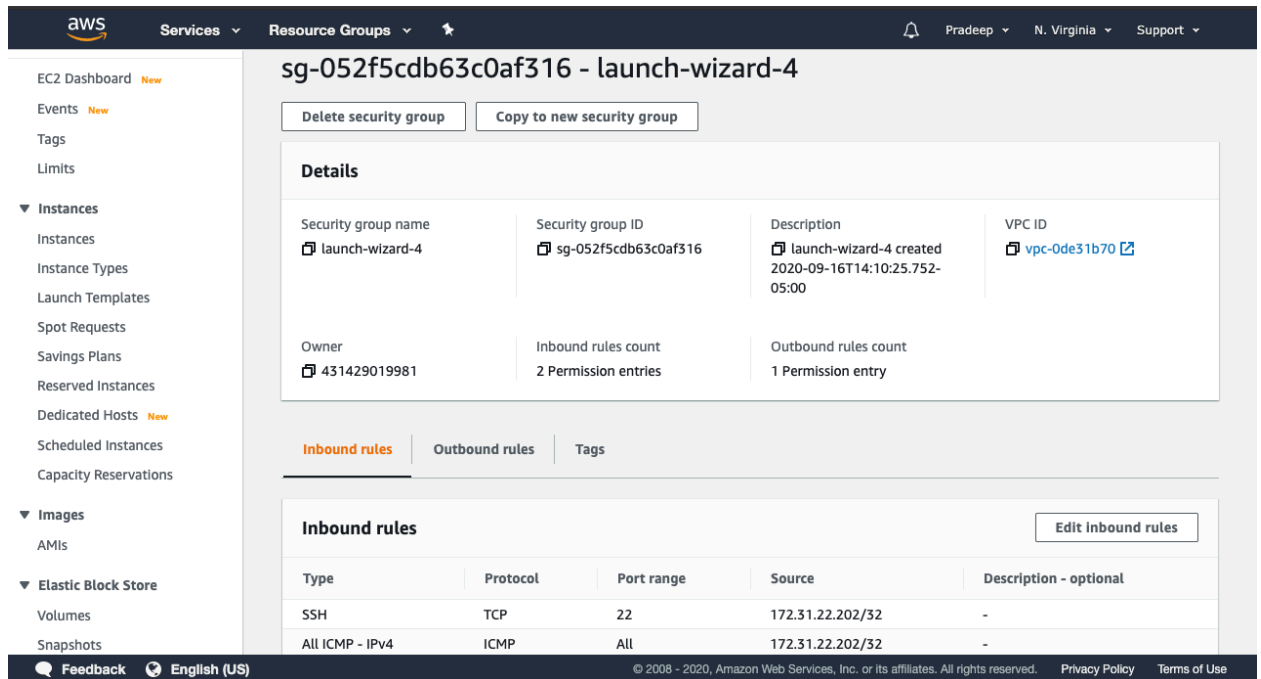
e) The screenshot of the Security group that shows the rules for incoming traffic of the 2nd EC2 (2)



The screenshot displays the AWS Management Console interface for a Security Group. The left sidebar shows navigation options like EC2 Dashboard, Events, Tags, Limits, Instances, Images, and Elastic Block Store. The main content area shows the details for Security Group **sg-06f7a74beca70154e - launch-wizard-3**. It includes buttons for "Delete security group" and "Copy to new security group". The "Details" section provides information about the security group name, ID, description, VPC ID, owner, and rule counts. Below this, the "Inbound rules" tab is selected, showing a table of inbound rules.

Type	Protocol	Port range	Source	Description - optional
SSH	TCP	22	0.0.0.0/0	-
All ICMP - IPv4	ICMP	All	64.189.205.232/32	-

f) The screenshot of the Security group that shows the rules for incoming traffic of the 3rd EC2 (2)



The screenshot displays the AWS Management Console interface for a Security Group. The left sidebar shows navigation options like EC2 Dashboard, Events, Tags, Limits, Instances, Images, and Elastic Block Store. The main content area shows the details for Security Group **sg-052f5cdb63c0af316 - launch-wizard-4**. It includes buttons for "Delete security group" and "Copy to new security group". The "Details" section provides information about the security group name, ID, description, VPC ID, owner, and rule counts. Below this, the "Inbound rules" tab is selected, showing a table of inbound rules.

Type	Protocol	Port range	Source	Description - optional
SSH	TCP	22	172.31.22.202/32	-
All ICMP - IPv4	ICMP	All	172.31.22.202/32	-

Problem 2 (12):

a) Test connectivity using the ping command (6). Think why some can connect and some can not.

Use internal IP address	1 st EC2	2 nd EC2	3 rd EC2
1 st EC2	Y	N	Y
2 nd EC2	Y	Y	N
3 rd EC2	Y	N	Y
Your laptop	N	N	N

b) Test connectivity using the ping command (6). Think why some can connect and some can not.

Use external IP address	1 st EC2	2 nd EC2	3 rd EC2
1 st EC2	Y	N	N(no public ip)
2 nd EC2	Y	N	N(no public ip)
3 rd EC2	N	N	N(no public ip)
Your laptop	Y	Y	N(no public ip)