Course: SBL: Cloud Computing
Course code: CSL605
Year: TE SEM: VI

Experiment No. 07
AIM:-To study and Implement Security as a Service on AWS
Name:
Roll Number:
Date of Performance:
Date of Submission:

Evaluation

Performance Indicator	Max. Marks	Marks Obtained
Performance	5	
Understanding	5	
Journal work and timely submission.	10	
Total	**20**	

Performance Indicator	Exceed Expectations (EE)	Meet Expectations (ME)	Below Expectations (BE)
Performance	5	3	2
Understanding	5	3	2
Journal work and timely submission.	10	8	4

Checked by

Name of Faculty : **Ichhanshu Jaiswal**

Signature :

Date :

Experiment No. 7

Aim: To study and Implement Security as a Service on AWS

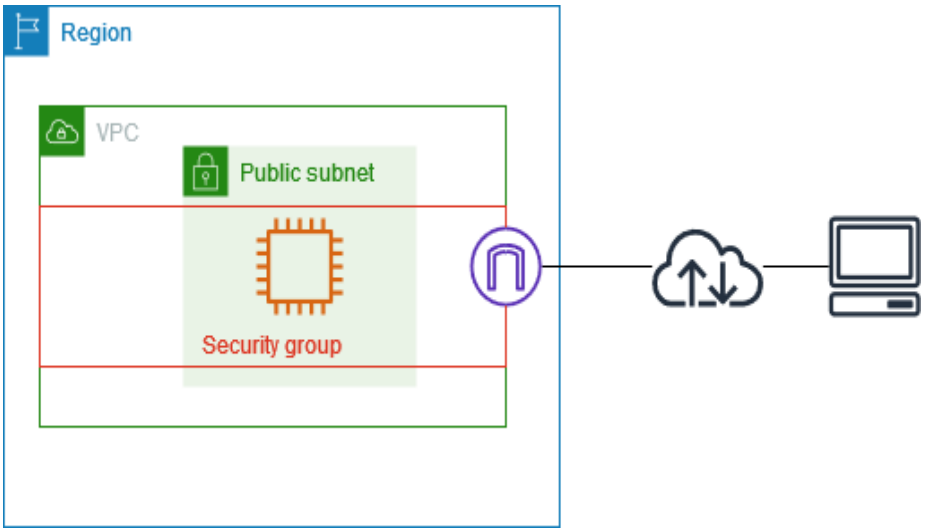
Theory:

In Amazon Web Services (AWS), a security group is like having bodyguards for your virtual machines (EC2 instances) in the cloud. These bodyguards protect your instances by controlling who can come in (inbound) and who can go out (outbound).

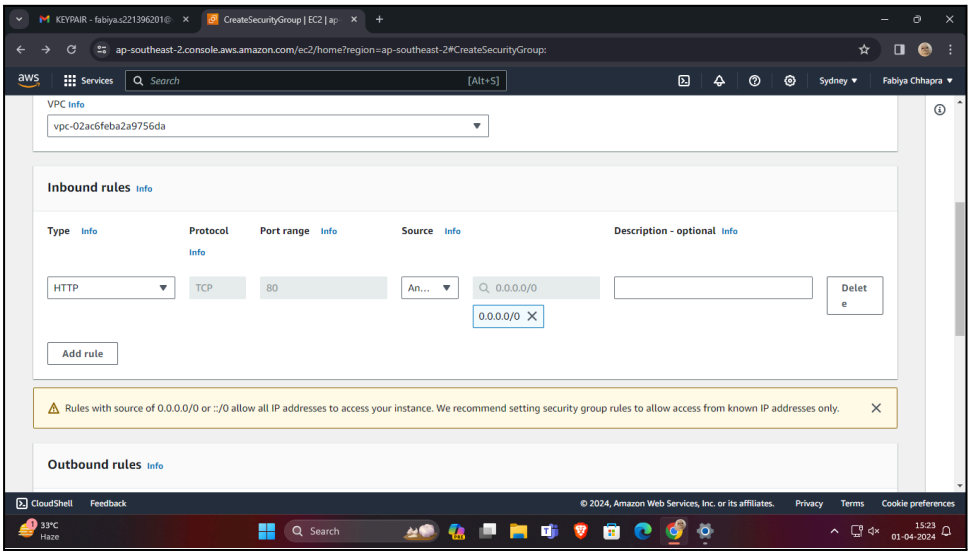
Security Group :- It's a set of rules that controls inbound and outbound traffic to and from your EC2 instances.

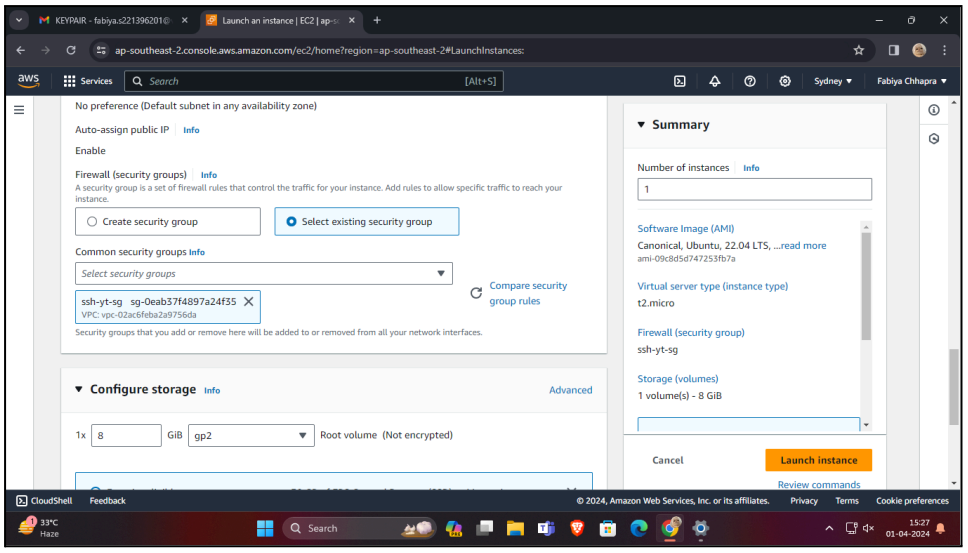
- Inbound Rules: These rules dictate who can enter your party (or access your EC2 instance). For instance, you might allow web traffic on port 80 or secure connections on port 443. In real life, these are like specifying that only guests with valid invitations can come inside your party.

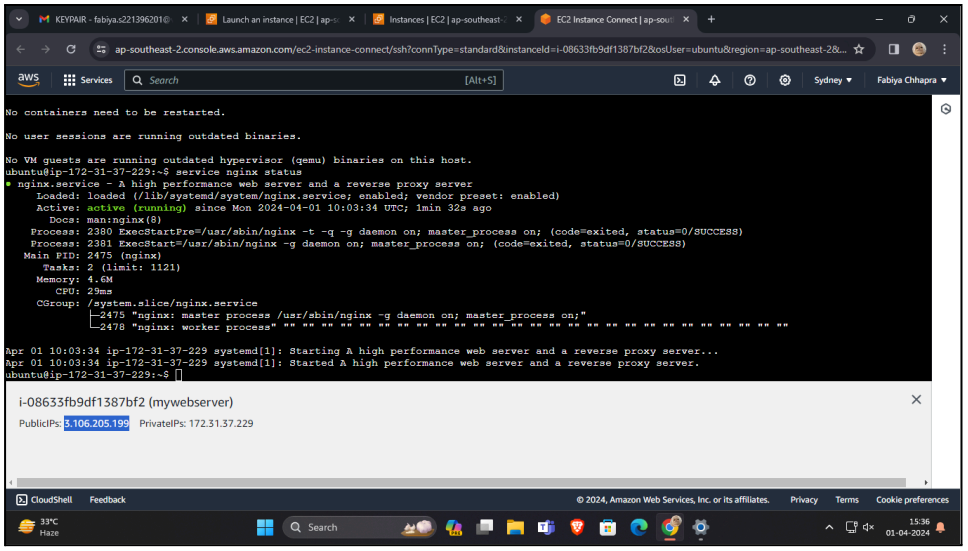
- Outbound Rules: These rules determine where your guests (or your EC2 instance) can go. For example, you might allow your guests to leave and return but not take strangers with them. In AWS, this is akin to allowing your EC2 instance to connect to specific services or websites but not just anywhere on the internet.

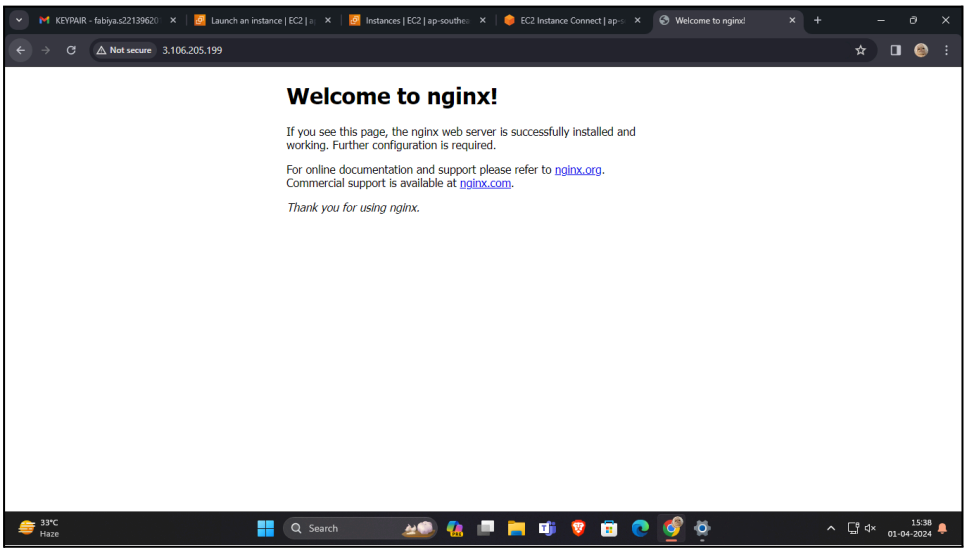


Output:


KEYPAIR - fabiya.s221396201@
CreateSecurityGroup | EC2 | ap
ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#CreateSecurityGroup:
Services
Search
[Alt+S]
Sydney
Fabiya Chhapra
VPC Info
vpc-02ac6feba2a9756da
Inbound rules Info
Type Info
Protocol Info
Port range Info
Source Info
Description - optional Info
HTTP
TCP
80
An...
0.0.0.0/0
0.0.0.0/0
Delet e
Add rule
Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Outbound rules Info
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
33°C
Haze
Search
15:23
01-04-2024


KEYPAIR - fabiya.s221396201@
Launch an instance | EC2 | ap-s
ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#LaunchInstances:
Services
Search
[Alt+S]
Sydney
Fabiya Chhapra
No preference (Default subnet in any availability zone)
Auto-assign public IP Info
Enable
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
Common security groups Info
Select security groups
ssh-yt-sg sg-0eab37f4897a24f35
VPC: vpc-02ac6feba2a9756da
Compare security group rules
Security groups that you add or remove here will be added to or removed from all your network interfaces.
Configure storage Info
Advanced
1x
8
GiB
gp2
Root volume (Not encrypted)
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-09c8d5d747253fb7a
Virtual server type (instance type)
t2.micro
Firewall (security group)
ssh-yt-sg
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
33°C
Haze
Search
15:27
01-04-2024





Conclusion: Comment on multiple security groups for a single instance