SECURITY GROUPS AND NACL IN AWS

cybersecurity has grown to be a crucial component of any business in the modern digital age. Access management is a fundamental element of cybersecurity. Controlling access includes deciding who has access to what resources and for what goals. The management of resource access in the cloud is done using security groups. We shall define security groups in this article and explain how they operate and may be created in Amazon Web Services (AWS). We'll also define a few crucial terms related to security groups, offer pertinent examples, and give step-by-step directions with screenshots.

An example of one of these features is the security group, which functions as a virtual firewall to regulate the inbound and outgoing traffic for Amazon EC2 instances or other AWS resources in a VPC. We shall go over a security group's definition and formation in this article.

1. **Security Group: It performs the function of a virtual firewall, managing the inbound and outbound traffic for one or more Amazon EC2 instances or other AWS services within a VPC.**
2. **Inbound Rules: These outline the types of traffic that are permitted to use the resources. It serves as a virtual firewall, controlling the traffic going in and coming out of a VPC for one or more Amazon EC2 instances or other AWS services.**
3. **Outbound Rules: These regulate the traffic that is permitted to depart from the resources. The destination for incoming traffic is dealt with by outbound rules. They may be forwarded to an alternative Security Group, a CIDR block, a single IPv4 or IPv6 address, or all three.**
4. **Amazon EC2: A web service called Amazon Elastic Compute Cloud offers scalable computation capability in the cloud. For developers, it is intended to make web-scale cloud computing simpler.**
5. **VPC: A virtual network called a virtual private cloud enables you to launch Amazon resources into a defined virtual network.**
6. **CIDR: A technique for allocating IP addresses and rerouting Internet Protocol packets is called classless inter-domain routing (CIDR).**
7. **Protocol: A protocol is a collection of guidelines that controls how two devices communicate with one another.**
8. **Port: A port on a computer serves as the communication endpoint for a particular process or service.**

Steps to Create a Security Group

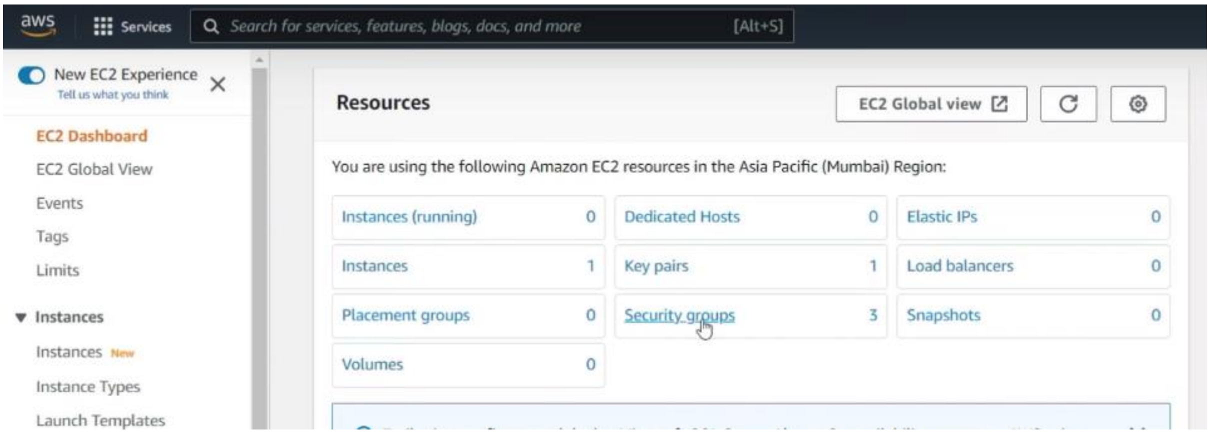
Let's talk about how to form a security group in AWS now that we have identified certain critical terms.

Step1: Access the EC2 Dashboard

Begin by logging into the Amazon Management Console. Navigate to the AWS console and sign in with your account credentials.

Step 2: Navigate to Security Groups

From the AWS console, go to the EC2 dashboard. On the left-hand panel, locate and select the "Security Groups" option.



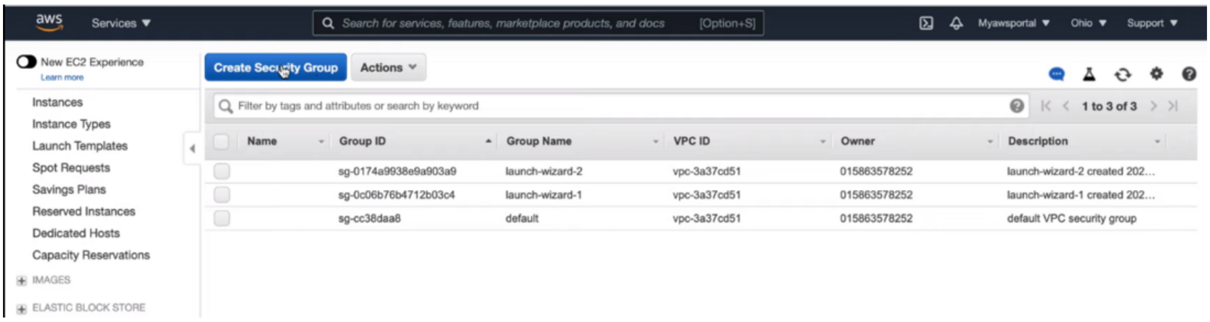
Resources

You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) Region:

Instances (running)	0	Dedicated Hosts	0	Elastic IPs	0
Instances	1	Key pairs	1	Load balancers	0
Placement groups	0	Security groups	3	Snapshots	0
Volumes	0				

Step 3: Initiate Security Group Creation

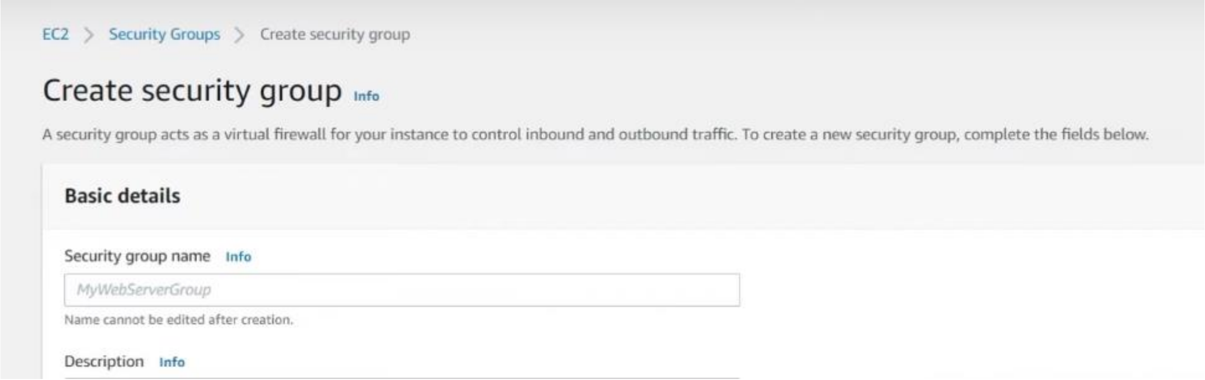
Within the "Security Groups" section, click on the "Create Security Group" button to start the creation process.



Name	Group ID	Group Name	VPC ID	Owner	Description
	sg-0174a9938e9a903a9	launch-wizard-2	vpc-3a37cd51	015863578252	launch-wizard-2 created 202...
	sg-0c06b76b4712b03c4	launch-wizard-1	vpc-3a37cd51	015863578252	launch-wizard-1 created 202...
	sg-cc38daa8	default	vpc-3a37cd51	015863578252	default VPC security group

Step 4: Define Security Group Details

Provide the necessary details for your security group. Enter a descriptive name and a brief description. Specify the Virtual Private Cloud (VPC) where the security group will reside.



Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info

MyWebServerGroup

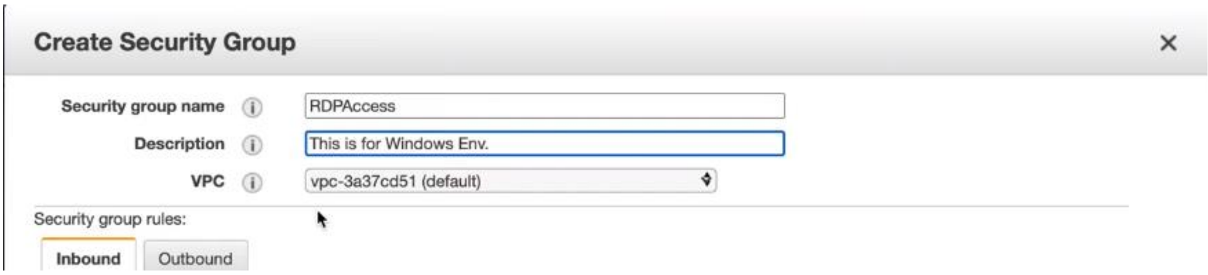
Name cannot be edited after creation.

Description Info

Insert your security group's information, including its name, description, and VPC. For your security group, you must also provide inbound and outgoing rules.

Step 5: Configure Inbound Rules

To define inbound rules, select the "Inbound Rules" tab and click on the "Add Rule" button. Configure each rule by specifying the protocol, port range, source IP address or range, and a description.



Security group name: RDPAccess

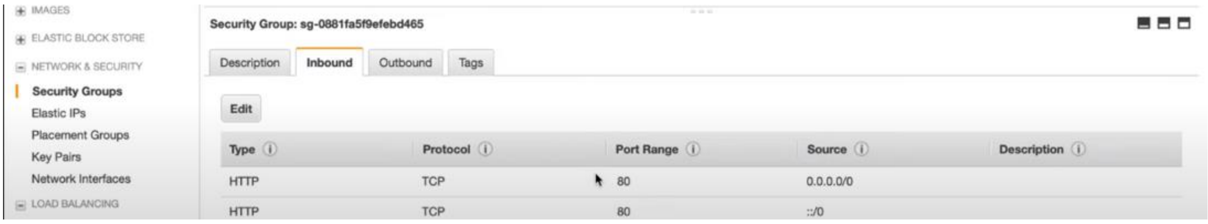
Description: This is for Windows Env.

VPC: vpc-3a37cd51 (default)

Security group rules:

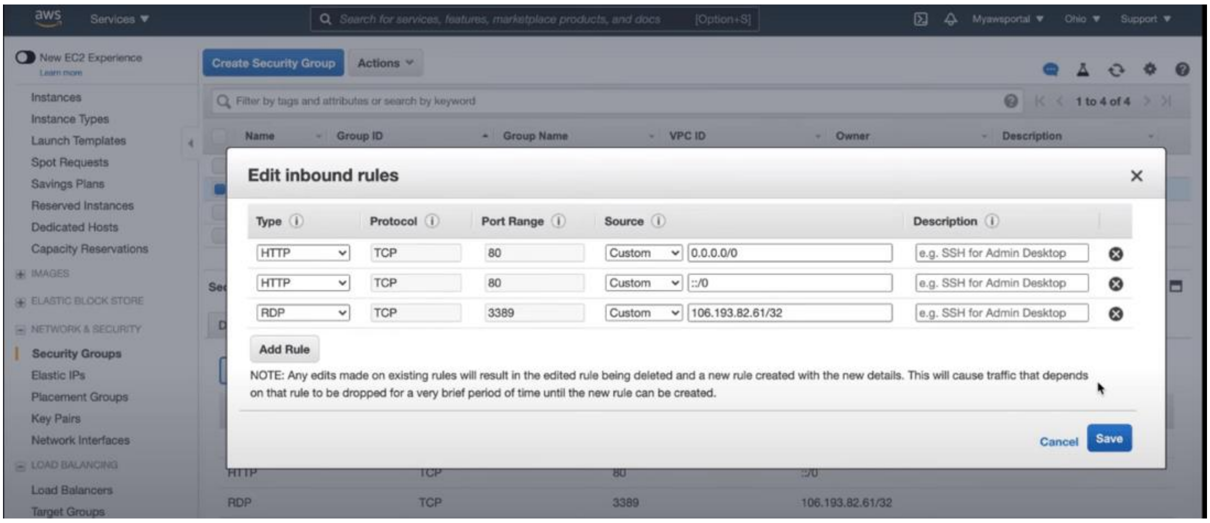
Step 6: Configure Outbound Rules

Similarly, configure outbound rules by selecting the "Outbound Rules" tab and clicking on the "Add Rule" button. Define the protocol, port range, destination IP address, and a description for each rule.



Security Group: sg-0881fa5f9efebd465

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	
HTTP	TCP	80	::/0	

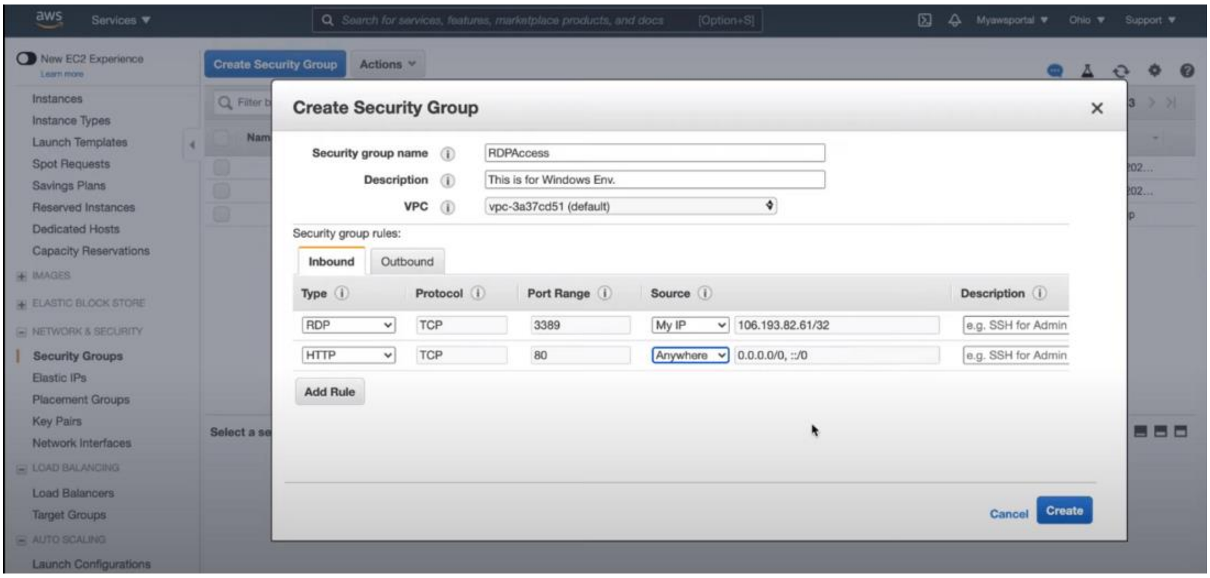


Type	Protocol	Port Range	Source		Description
HTTP	TCP	80	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
HTTP	TCP	80	Custom	::/0	e.g. SSH for Admin Desktop
RDP	TCP	3389	Custom	106.193.82.61/32	e.g. SSH for Admin Desktop

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Step 7: Review and Create

Carefully review all the configurations and rules you have set up. Once satisfied, click on the "Create Security Group" button to finalize and create your security group.



Create Security Group

Security group name: RDPAccess

Description: This is for Windows Env.

VPC: vpc-3a37cd51 (default)

Security group rules:

Inbound | Outbound

Type	Protocol	Port Range	Source		Description
RDP	TCP	3389	My IP	106.193.82.61/32	e.g. SSH for Admin
HTTP	TCP	80	Anywhere	0.0.0.0/0, ::/0	e.g. SSH for Admin

- **Note: Inbound and outbound security Group Rules comprise four different fields: Source, Protocol, Port Range & Description.**

- **Source: Typically, this is a private IP address, a subnet mask, or another security group. If you use the “anywhere (0.0.0.0/0)” option, you can also allow access to the entire internet. The everywhere (0.0.0.0/0) value must only be used when necessary, and you should be well aware of the risks involved.**

- **Protocol: TCP is usually the default protocol and is often greyed out. But you can adjust the protocols if you’re using specially-made rules that you wrote.**

- **Port Range: Usually, port ranges are pre-filled. Still, you have the option to choose a custom port range of your choice.**

- **Description: You can add a description to the rule you’ve generated in this area. The more specific you are, the better.**

Amazon EC2 security groups for Linux instances

Amazon EC2 security groups play a pivotal role in safeguarding Linux instances hosted on the Amazon Web Services (AWS) cloud platform. They serve as virtual firewalls, controlling inbound and outbound traffic to and from EC2 instances. Understanding how to configure and manage security groups is essential for maintaining a secure and efficient computing environment. In this detailed guide, we’ll delve into the intricacies of Amazon EC2 security groups for Linux instances.

Understanding EC2 Security Groups:

- **Definition: EC2 security groups act as virtual firewalls that regulate traffic to and from EC2 instances. They control inbound traffic (incoming data) and outbound traffic (outgoing data) based on defined rules.**

- **Stateful Filtering: Security groups operate on a stateful filtering paradigm, meaning that responses to allowed inbound traffic are automatically allowed, regardless of outbound rules. This simplifies configuration and ensures that return traffic is permitted.**

- **Default Rules: By default, all inbound traffic is denied, and all outbound traffic is allowed. You must explicitly define inbound rules to permit traffic to your instances. Outbound traffic is automatically allowed unless specific restrictions are imposed.**

Change, or Delete Security Groups

Managing security groups in AWS is a crucial aspect of maintaining a secure and compliant cloud environment. Whether you need to update rules, modify associations, or remove unused security groups, the process is straightforward. Here’s a simple guide on how to change or delete security groups in AWS:

Changing Security Groups:

- **Access the AWS Management Console: Log in to the AWS Management Console and navigate to the EC2 dashboard.**
- **Locate Security Groups: From the EC2 dashboard, select the “Security Groups” option from the navigation pane to view all existing security groups.**
- **Identify Target Security Group: Identify the security group you wish to modify and click on its name to access its configuration details.**
- **Update Security Group Rules: Within the security group details, navigate to the “Inbound” or “Outbound” rules tab to modify existing rules. Click on the “Edit” button to make changes, such as adding new rules, modifying existing ones, or removing unnecessary rules.**
- **Review and Apply Changes: Carefully review the updated rules to ensure they align with your security requirements. Once satisfied, click on the “Save” or “Apply Changes” button to implement the modifications.**

Deleting Security Groups:

- **Access the AWS Management Console: Follow the same initial steps to access the EC2 dashboard in the AWS Management Console.**
- **Locate Security Groups: From the EC2 dashboard, select the “Security Groups” option to view a list of all existing security groups.**
- **Identify Target Security Group: Identify the security group you intend to delete from the list of available security groups.**
- **Initiate Deletion: Select the target security group and click on the “Actions” dropdown menu. Choose the “Delete Security Group” option from the available actions.**
- **Confirm Deletion: AWS will prompt you to confirm the deletion of the selected security group. Review the details and implications of the deletion carefully.**
- **Confirm Deletion: If you’re certain you want to proceed with the deletion, click on the “Yes, Delete” button to confirm. Otherwise, you can cancel the operation to retain the security group.**

Conclusion

Security groups are a fundamental security feature in AWS, allowing you to control the traffic that is allowed to access your resources. In this article, we have discussed what a security group is and how to create it. By following the steps mentioned above, you can create security groups for your resources and ensure they are secure.

- **NACL: NACL stands for Network Access Control Lists.**
- **It is a security layer for your VPC that controls the traffic in and out of one or more subnets.**
- **It is an optional layer for your VPC.**

- You can set up a Network ACL similar to the security group that adds an additional layer of security to your VPC.

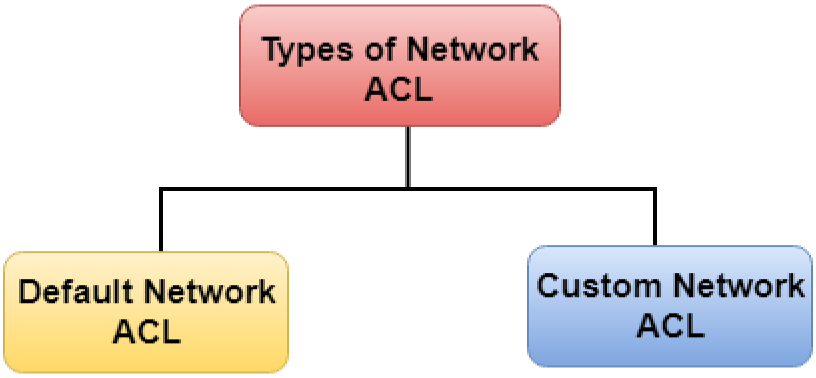
Some important related to Network ACL:

- Your custom VPC automatically comes with the default Network ACL which includes all inbound and outbound ipv4 traffic.
- You can also create a custom network ACL and associates with a subnet. By default, a custom Network ACL denies all the inbound and outbound ipv4 traffic until you add rules.
- If you do not explicitly create Network ACL, then the default Network ACL automatically associated with the subnet.
- You can associate multiple subnets with a Network ACL. However, a subnet can be associated with the single Network ACL at a time.
- Network ACL is associated with both inbound and outbound rules that can either deny or allow the rules.
- A Network ACL contains numbered lists of rules that are evaluated in order, starting from the lowest numbered rule, to determine whether the traffic goes in or out of the subnet associated with the Network ACL. The highest numbered rule can be 32766. It is recommended to create new rules with increments (For example, increments of 10 or 100) so that you can easily add new rules where you need later on.

Network ACL Components

The following are the components of a Network ACL:

- Rule number: Rule number is a number associated with every rule. Rules are evaluated starting with the lowest-numbered rule. As soon as the rule matches traffic, the rule is applied regardless of whether the highest-numbered rule contradicts to it.
- Protocol: You can specify any protocol that has a standard protocol number. For example, Http, Https, ICMP, SSH, etc.
- Inbound rules: It specifies the source of the traffic and the destination port.
- Outbound rules: It specifies the destination traffic and destination port.



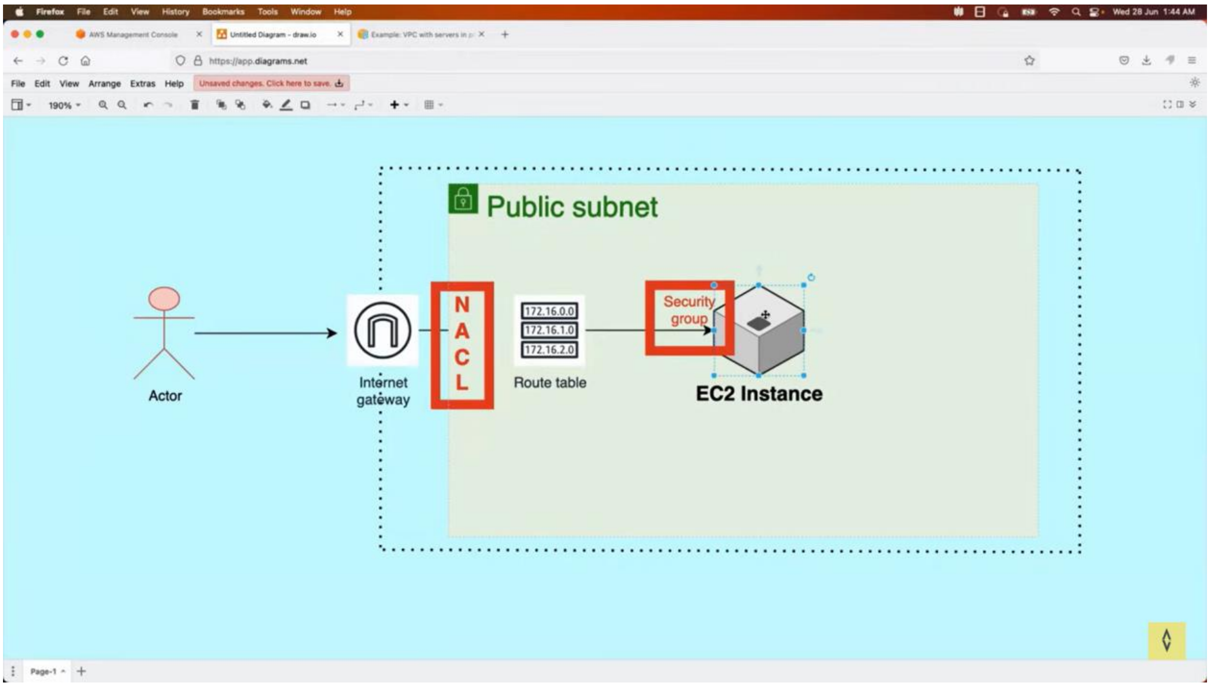
Types of Network ACL

There are two types of Network ACL:

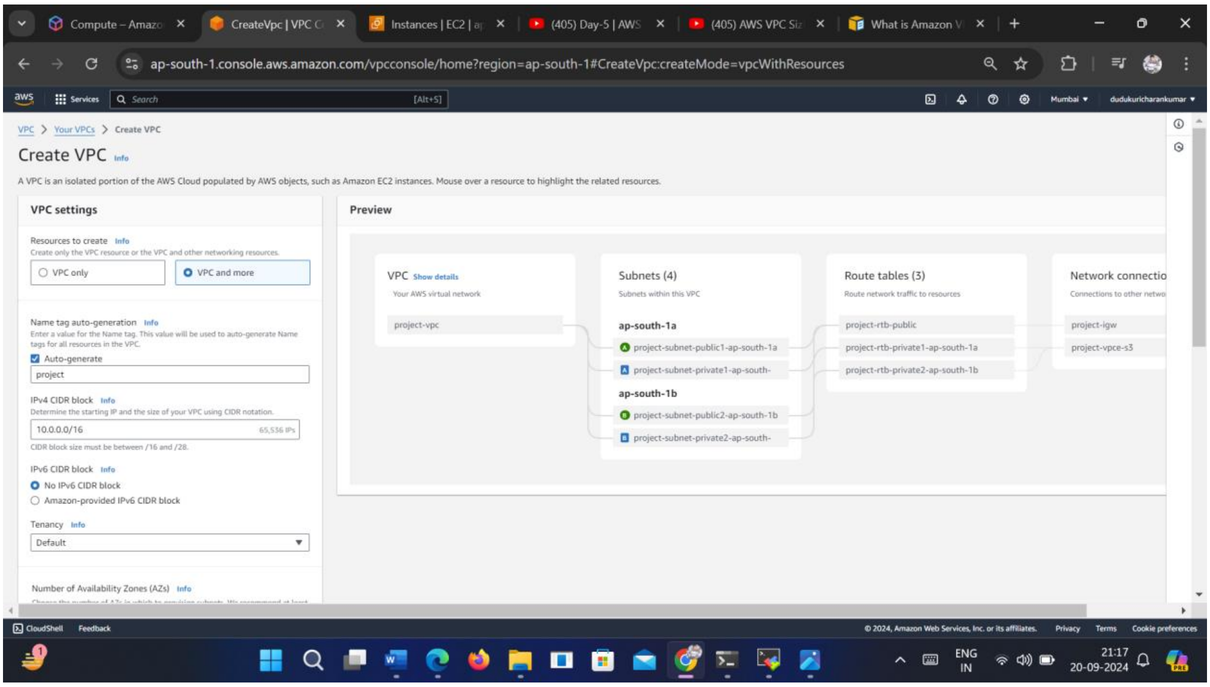
- Custom Network ACL
- Default Network ACL

Default Network ACL

The default Network ACL allows all the traffic to flow in or out of the subnet which is associated with it. Each Network ACL also includes a rule whose rule number is asterisk which determines if traffic does not match any of the numbered rules, then it is denied. This rule cannot be modified or removed.



STEP 1: Search for vpc in console



ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateVpc:createMode=vpcWithResources

VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
○ VPC only ● VPC and more

Name tag auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.
☑ Auto-generate
project

IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.
10.0.0.0/16 65,536 IPs
CIDR block size must be between /16 and /28.

IPv6 CIDR block Info
● No IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block

Tenancy Info
Default

Number of Availability Zones (AZs) Info

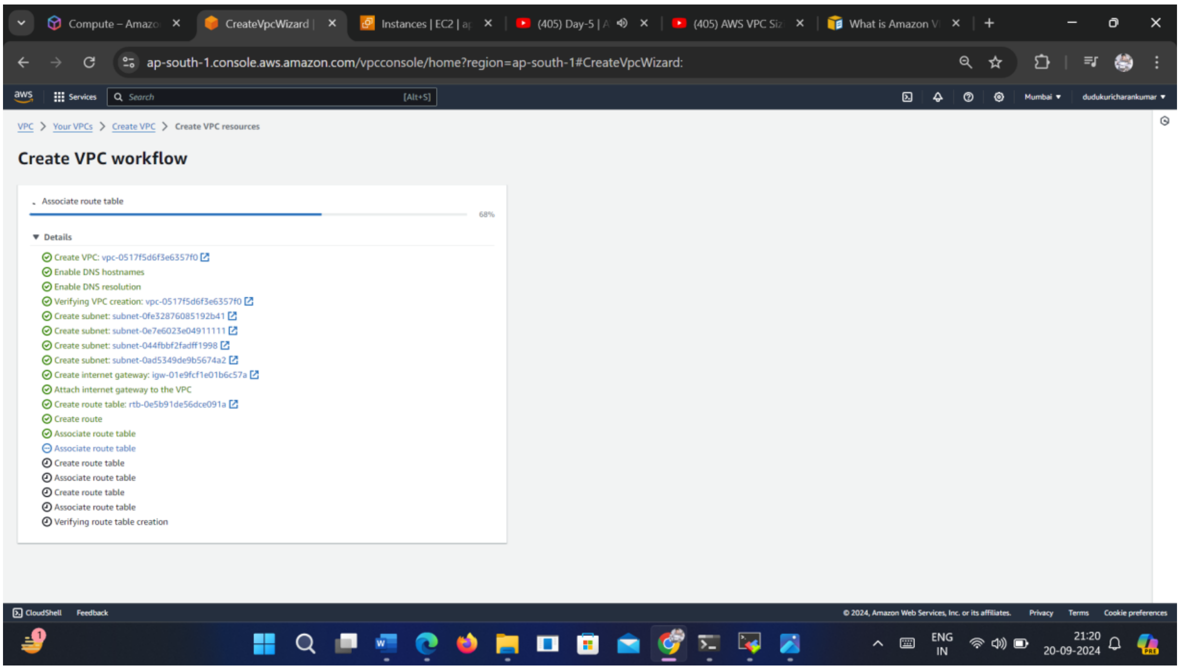
Preview

VPC Show details
Your AWS virtual network
project-vpc

Subnets (4)
Subnets within this VPC
ap-south-1a
project-subnet-public1-ap-south-1a
project-subnet-private1-ap-south-
ap-south-1b
project-subnet-public2-ap-south-1b
project-subnet-private2-ap-south-

Route tables (3)
Route network traffic to resources
project-rtb-public
project-rtb-private1-ap-south-1a
project-rtb-private2-ap-south-1b

Network connectio
Connections to other netwo
project-igw
project-vpce-s3

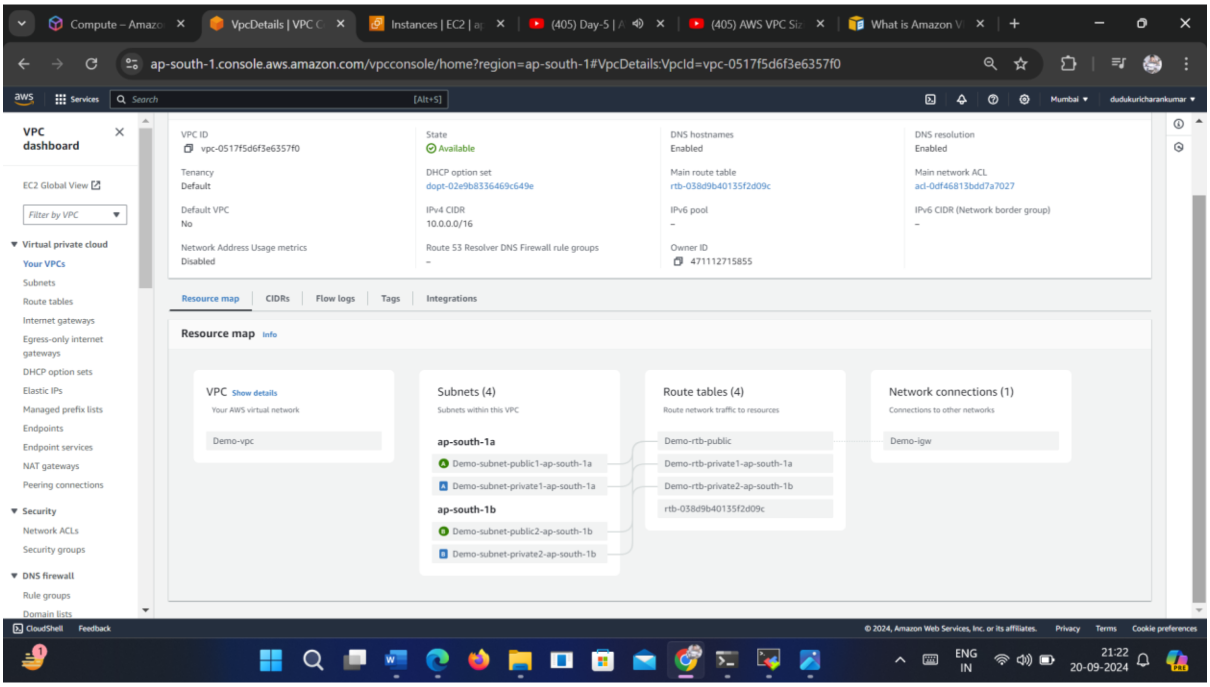


Create VPC workflow

Associate route table 68%

Details

- ✓ Create VPC: vpc-0517f5d6f3e6357f0
- ✓ Enable DNS hostnames
- ✓ Enable DNS resolution
- ✓ Verifying VPC creation: vpc-0517f5d6f3e6357f0
- ✓ Create subnet: subnet-0fe32876085192b41
- ✓ Create subnet: subnet-0e7e6023e04911111
- ✓ Create subnet: subnet-044fbbf2fadff1998
- ✓ Create subnet: subnet-0ad5349de9b5674a2
- ✓ Create internet gateway: igw-01e9fcf1e01b6c57a
- ✓ Attach internet gateway to the VPC
- ✓ Create route table: rtb-0e5b91de56dce091a
- ✓ Create route
- ✓ Associate route table
- Associate route table
- Create route table
- Associate route table
- Create route table
- Associate route table
- Verifying route table creation



VPC ID vpc-0517f5d6f3e6357f0	State ✓ Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-02e9b8336469c649e	Main route table rtb-038d9b40135f2d09c	Main network ACL acl-0df46813bdd7a7027
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool –	IPv6 CIDR (Network border group) –
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups –	Owner ID 471112715855	

Resource map Info

VPC Show details
Your AWS virtual network
- Demo-vpc

Subnets (4)
Subnets within this VPC

ap-south-1a
- Demo-subnet-public1-ap-south-1a
- Demo-subnet-private1-ap-south-1a

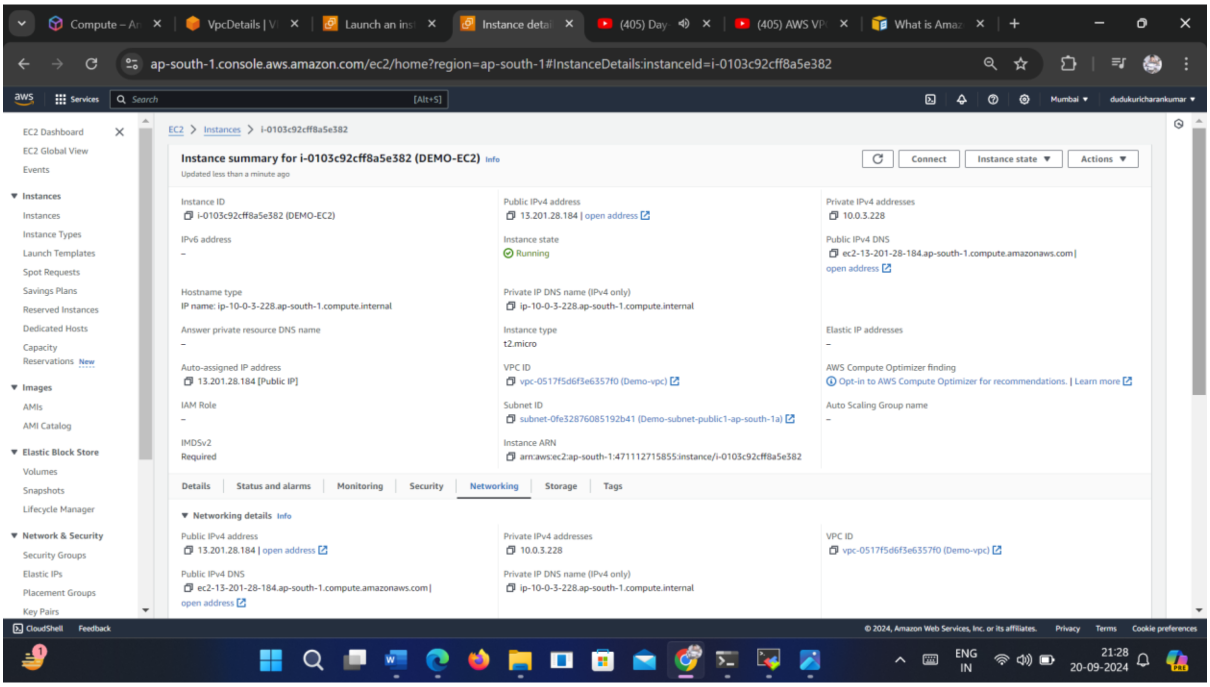
ap-south-1b
- Demo-subnet-public2-ap-south-1b
- Demo-subnet-private2-ap-south-1b

Route tables (4)
Route network traffic to resources
- Demo-rtb-public
- Demo-rtb-private1-ap-south-1a
- Demo-rtb-private2-ap-south-1b
- rtb-038d9b40135f2d09c

Network connections (1)
Connections to other networks
- Demo-igw

STEP 2:

CREATE EC2 INSTANCE



Instance summary for i-0103c92cff8a5e382 (DEMO-EC2) Info

Updated less than a minute ago

Instance ID: i-0103c92cff8a5e382 (DEMO-EC2)

Public IPv4 address: 13.201.28.184 | open address

Private IPv4 addresses: 10.0.3.228

IPv6 address: –

Instance state: Running

Public IPv4 DNS: ec2-13-201-28-184.ap-south-1.compute.amazonaws.com | open address

Hostname type: IP name: ip-10-0-3-228.ap-south-1.compute.internal

Private IP DNS name (IPv4 only): ip-10-0-3-228.ap-south-1.compute.internal

Answer private resource DNS name: –

Instance type: t2.micro

Elastic IP addresses: –

Auto-assigned IP address: 13.201.28.184 [Public IP]

VPC ID: vpc-0517f5d6f3e6357f0 (Demo-vpc)

AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations. | Learn more

IAM Role: –

Subnet ID: subnet-0fe32876085192b41 (Demo-subnet-public1-ap-south-1a)

Auto Scaling Group name: –

IMDSv2: Required

Instance ARN: arn:aws:ec2:ap-south-1:471112715855:instance/i-0103c92cff8a5e382

Networking details Info

Public IPv4 address: 13.201.28.184 | open address

Private IPv4 addresses: 10.0.3.228

VPC ID: vpc-0517f5d6f3e6357f0 (Demo-vpc)

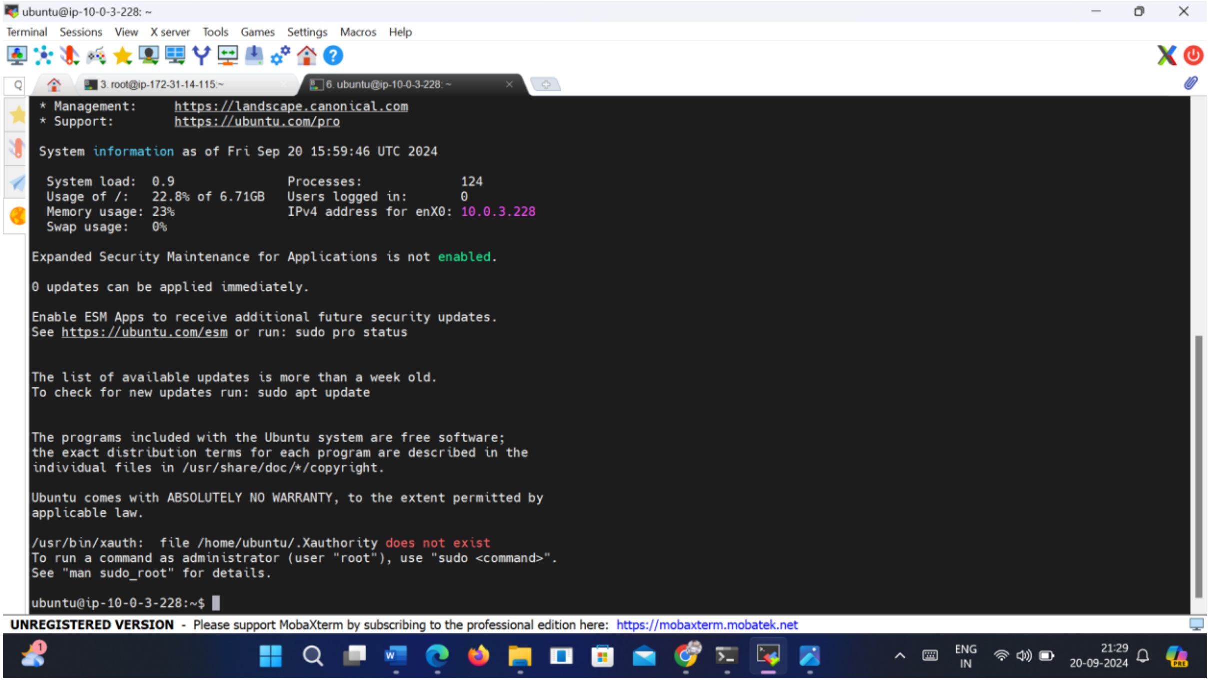
Public IPv4 DNS: ec2-13-201-28-184.ap-south-1.compute.amazonaws.com | open address

Private IP DNS name (IPv4 only): ip-10-0-3-228.ap-south-1.compute.internal

© 2024, Amazon Web Services, Inc. or its affiliates.

STEP 3:

CONNECT TO EC2 INSTANCE


ubuntu@ip-10-0-3-228: ~
Terminal Sessions View X server Tools Games Settings Macros Help
3. root@ip-172-31-14-115:~
6. ubuntu@ip-10-0-3-228: ~

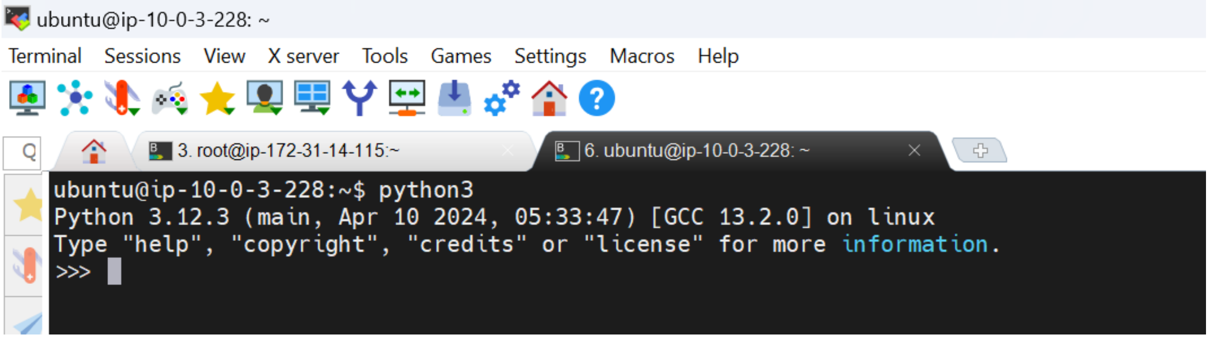
```
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Fri Sep 20 15:59:46 UTC 2024

  System load:  0.9               Processes:             124
  Usage of /:   22.8% of 6.71GB   Users logged in:       0
  Memory usage: 23%               IPv4 address for enX0: 10.0.3.228
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

/usr/bin/xauth:  file /home/ubuntu/.Xauthority does not exist
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-3-228:~$ 
```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

- **Update the packages**

STEP 4:

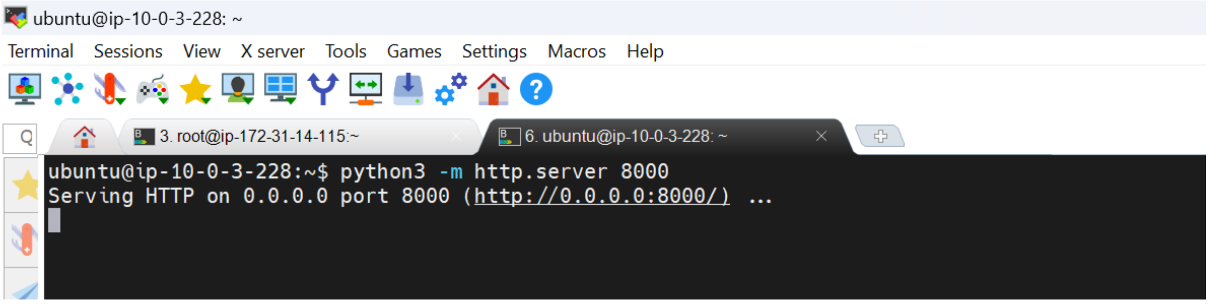
- **By default python is installed in server.**
- **Run the simple httpd server on python**



```
ubuntu@ip-10-0-3-228:~$ python3
Python 3.12.3 (main, Apr 10 2024, 05:33:47) [GCC 13.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

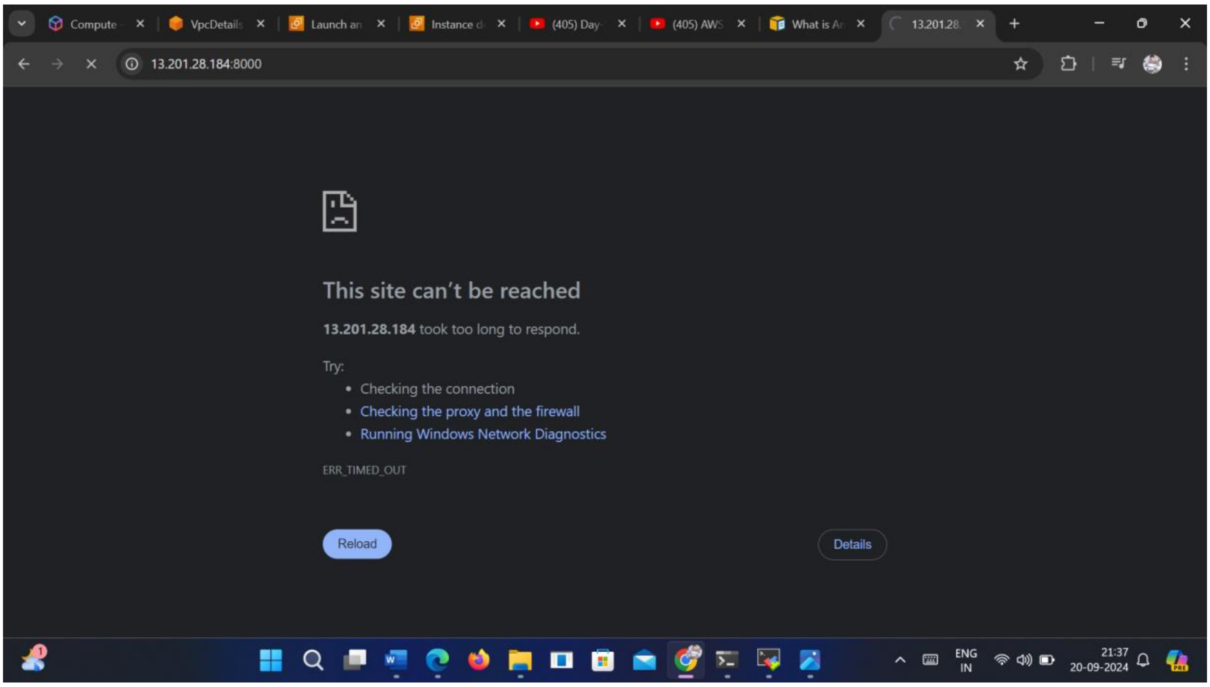
python3 -m http.server 8000

http server running on 8000 port



```
ubuntu@ip-10-0-3-228:~$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

- **Now I want access application using public_ip of server**



This site can’t be reached

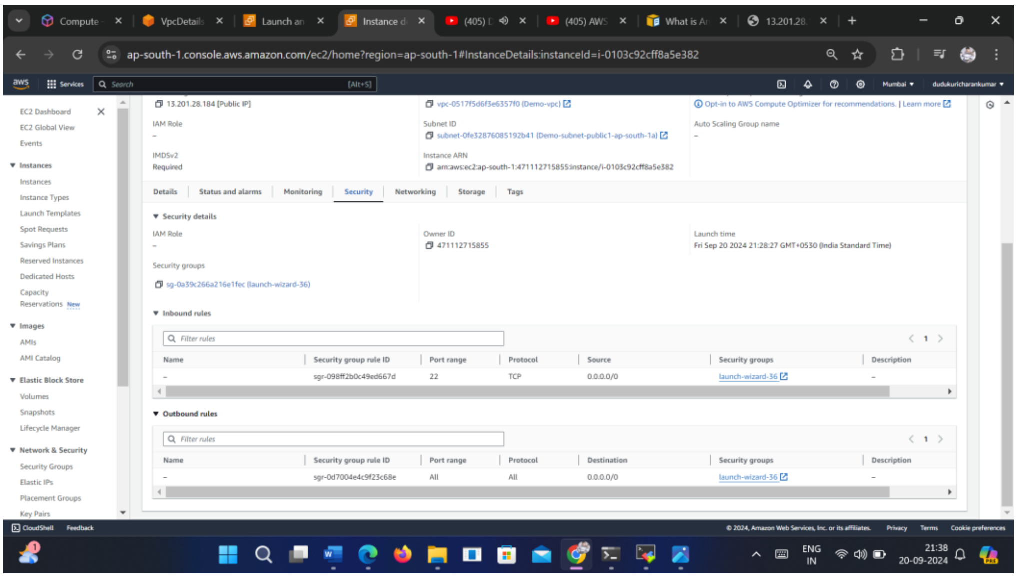
13.201.28.184 took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_TIMED_OUT

- **I didn’t access the application.Because by default AWS doesn’t ports in security groups**



ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#InstanceDetails:instanceId=i-0103c92cff8a5e382

13.201.28.184 [Public IP]

vpc-0517f5d6f3e6357f0 (Demo-vpc)

Opt-in to AWS Compute Optimizer for recommendations. | Learn more

IAM Role
–

Subnet ID
subnet-0fe32876085192b41 (Demo-subnet-public1-ap-south-1a)

Auto Scaling Group name
–

IMDSv2
Required

Instance ARN
arn:aws:ec2:ap-south-1:471112715855:instance/i-0103c92cff8a5e382

Security details

IAM Role
–

Owner ID
471112715855

Launch time
Fri Sep 20 2024 21:28:27 GMT+0530 (India Standard Time)

Security groups
sg-0a39c266a216e1fec (launch-wizard-36)

Inbound rules

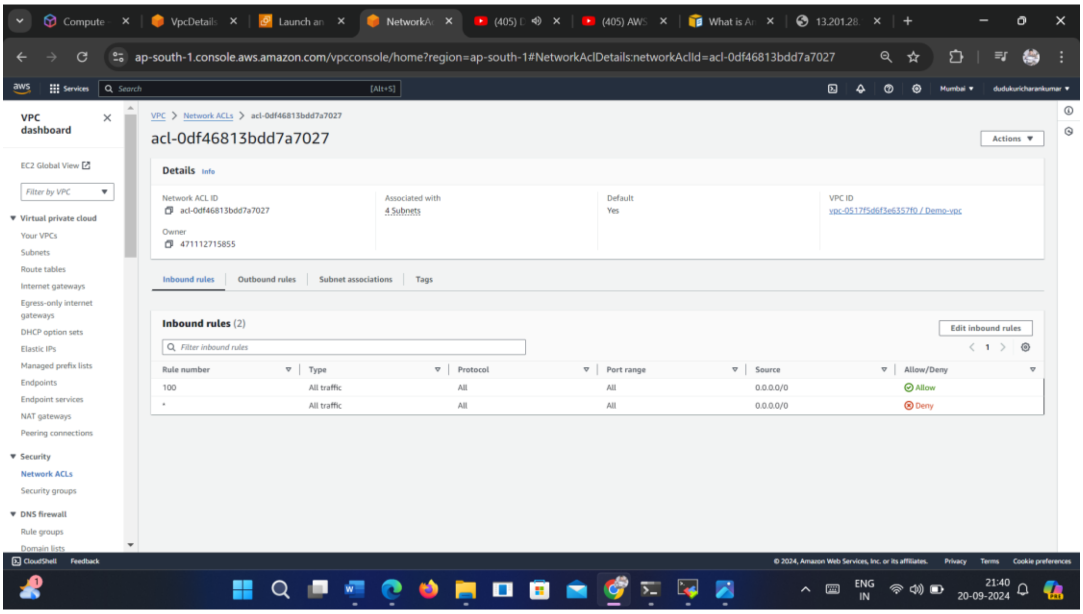
Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
–	sgr-098ff2b0c49ed667d	22	TCP	0.0.0.0/0	launch-wizard-36	–

Outbound rules

Name	Security group rule ID	Port range	Protocol	Destination	Security groups	Description
–	sgr-0d7004e4c9f23c68e	All	All	0.0.0.0/0	launch-wizard-36	–

- **By default Ec2 allows only one port 22**

NACL:



ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#NetworkAclDetails:networkAclId=acl-0df46813bdd7a7027

VPC > Network ACLs > acl-0df46813bdd7a7027

acl-0df46813bdd7a7027

Details

Network ACL ID
acl-0df46813bdd7a7027

Associated with
4 Subnets

Default
Yes

VPC ID
vpc-0517f5d6f3e6357f0 / Demo-vpc

Owner
471112715855

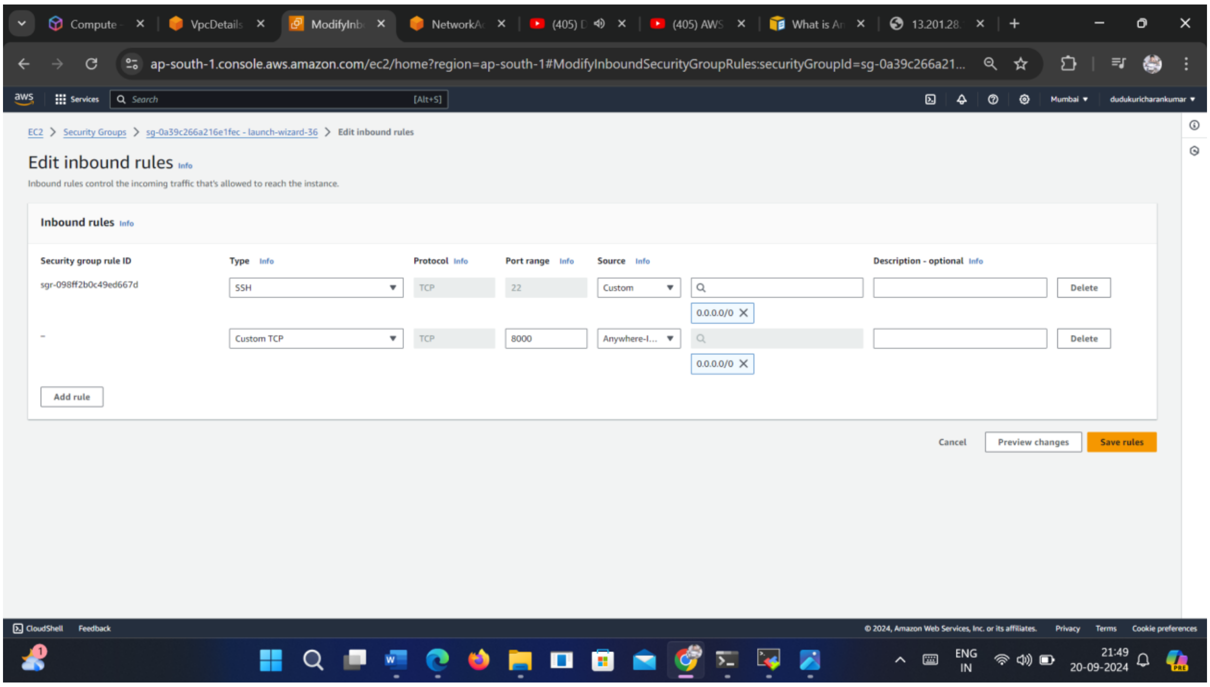
Inbound rules (2)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

- **NACL is a first layer of defence for entire subnet. In this it allows inbound all traffic**
- **It will verify rule number priority .The number which is highest as higher priority**
- **NACL allowing traffic but security groups restrict the request because we didn’t open the port 8000 in security groups.**

STEP 5:

Go to security groups and allow 8000 port.so that we can access it.



ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#ModifyInboundSecurityGroupRules:securityGroupId=sg-0a39c266a21...

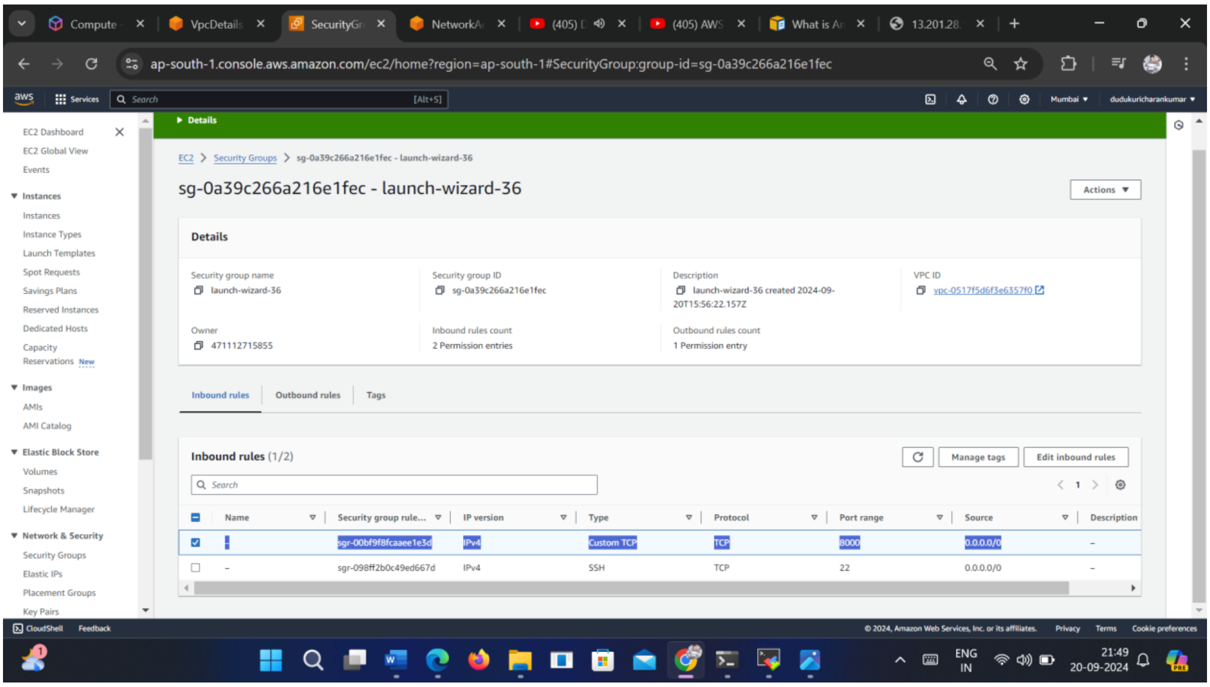
EC2 > Security Groups > sg-0a39c266a216e1fec - launch-wizard-36 > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type	Protocol	Port range	Source		Description - optional	
sgr-098ff2b0c49ed667d	SSH	TCP	22	Custom	0.0.0.0/0		Delete
-	Custom TCP	TCP	8000	Anywhere-I...	0.0.0.0/0		Delete



ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#SecurityGroup:group-id=sg-0a39c266a216e1fec

EC2 > Security Groups > sg-0a39c266a216e1fec - launch-wizard-36

sg-0a39c266a216e1fec - launch-wizard-36

Details

Security group name: launch-wizard-36

Security group ID: sg-0a39c266a216e1fec

Description: launch-wizard-36 created 2024-09-20T15:56:22.157Z

VPC ID: vpc-0517f5d6f3e6357f0

Owner: 471112715855

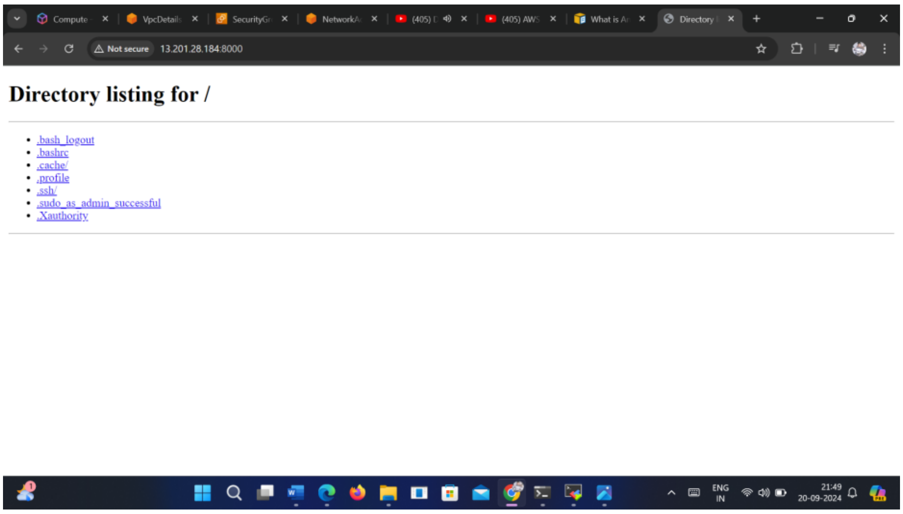
Inbound rules count: 2 Permission entries

Outbound rules count: 1 Permission entry

Inbound rules (1/2)

	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
☑		sgr-00bf9f8fcaaee1e3d	IPv4	Custom TCP	TCP	8000	0.0.0.0/0	–
□	–	sgr-098ff2b0c49ed667d	IPv4	SSH	TCP	22	0.0.0.0/0	–

Now http server is accessed.

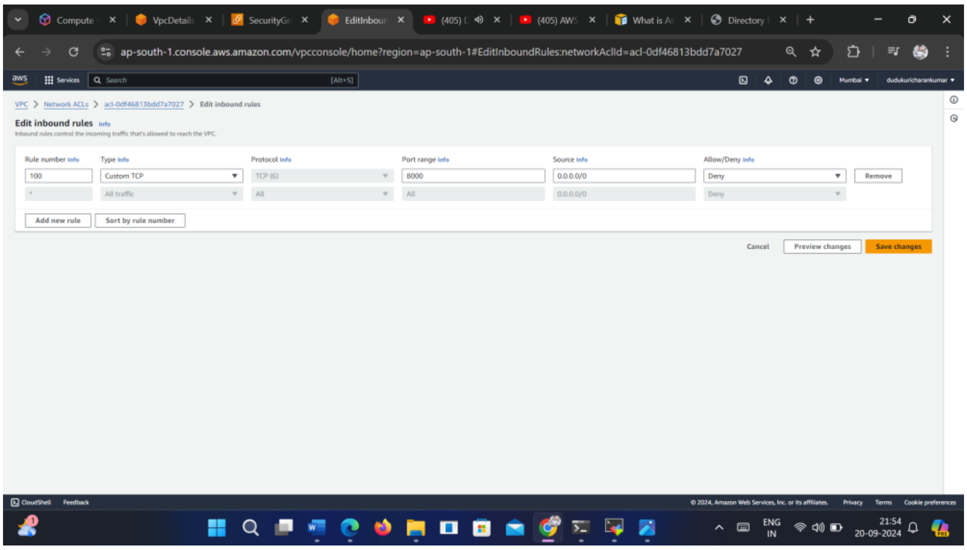


13.201.28.184:8000

Directory listing for /

- .bash_logout
- .bashrc
- .cache/
- .profile
- .ssh/
- .sudo_as_admin_successful
- .Xauthority

- **Now I changed inbound rule in NACL that 8000 port is blocked**



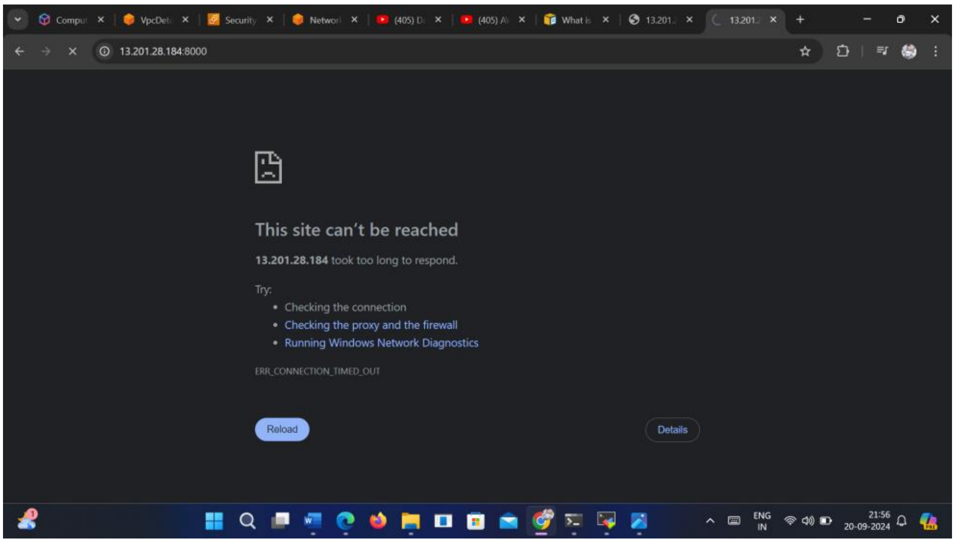
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#EditInboundRules:networkAclId=acl-0df46813bdd7a7027

VPC > Network ACLs > acl-0df46813bdd7a7027 > Edit inbound rules

Edit inbound rules

Inbound rules control the incoming traffic that's allowed to reach the VPC.

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	Custom TCP	TCP (6)	8000	0.0.0.0/0	Deny
*	All traffic	All	All	0.0.0.0/0	Deny



13.201.28.184:8000

This site can't be reached

13.201.28.184 took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

- **The http can’t be reached as I blocked the port number at Subnet level using NACL.Even 8000 port is opened in Security groups**.