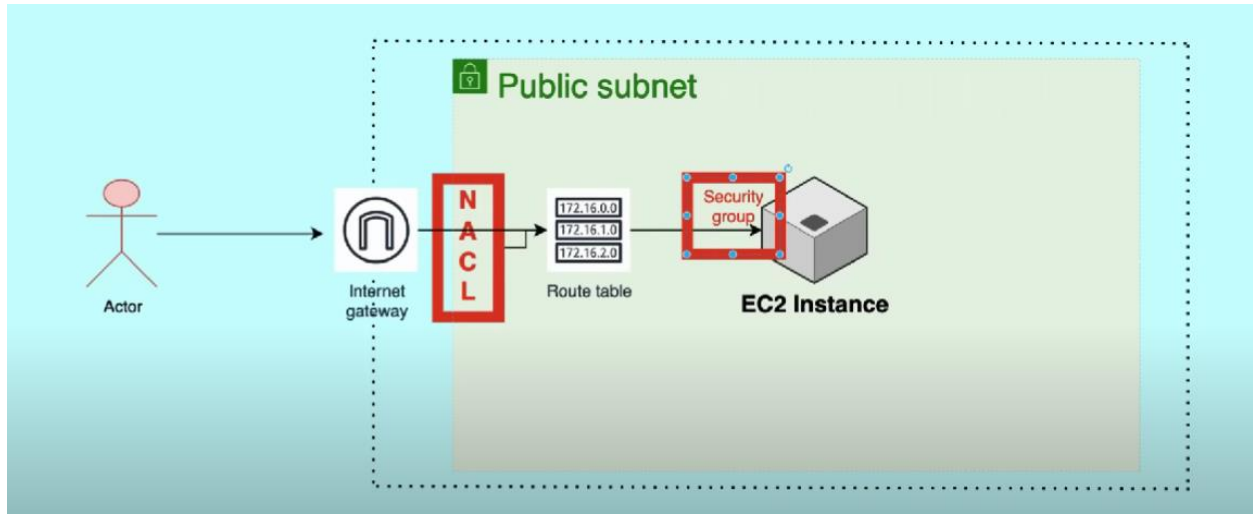
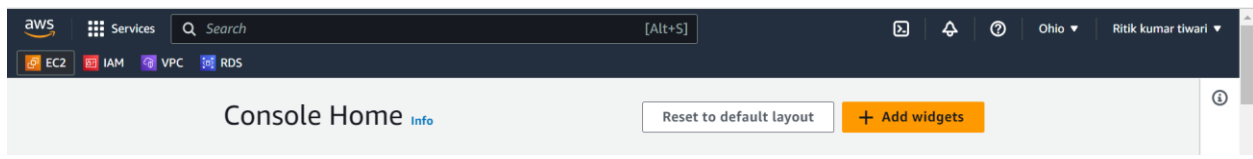


Hands-On Practical Note**

🔒🌐 **Unlock the Power of Security Groups and NACLs in AWS!** 🚀🔒

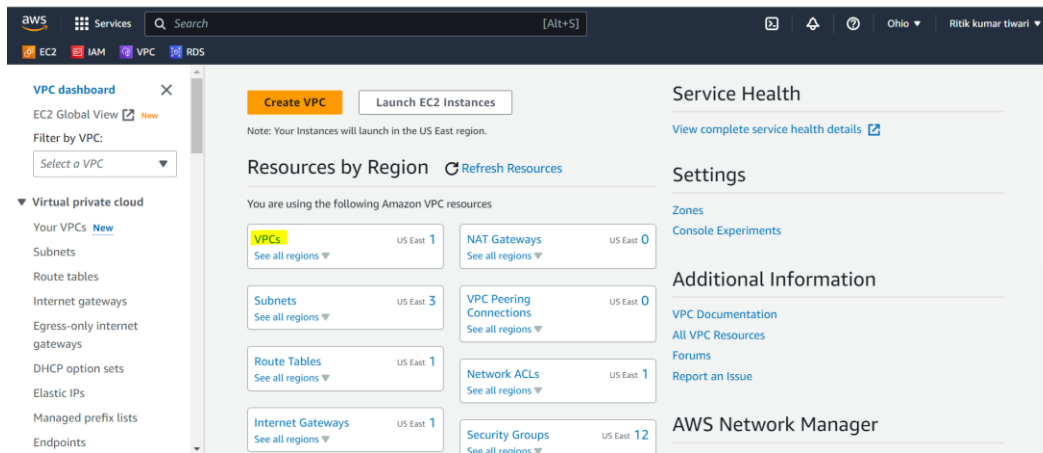


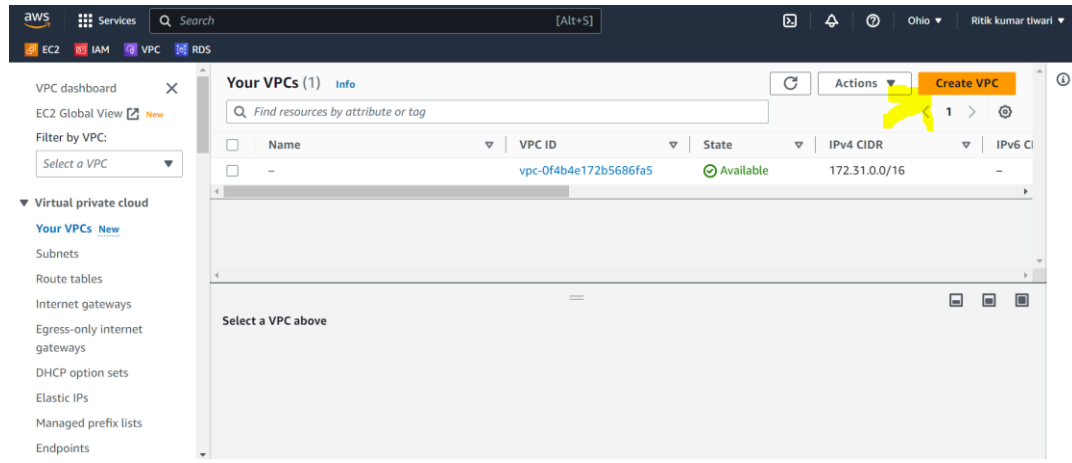
How to create VPC (Virtual private cloud):



1st.

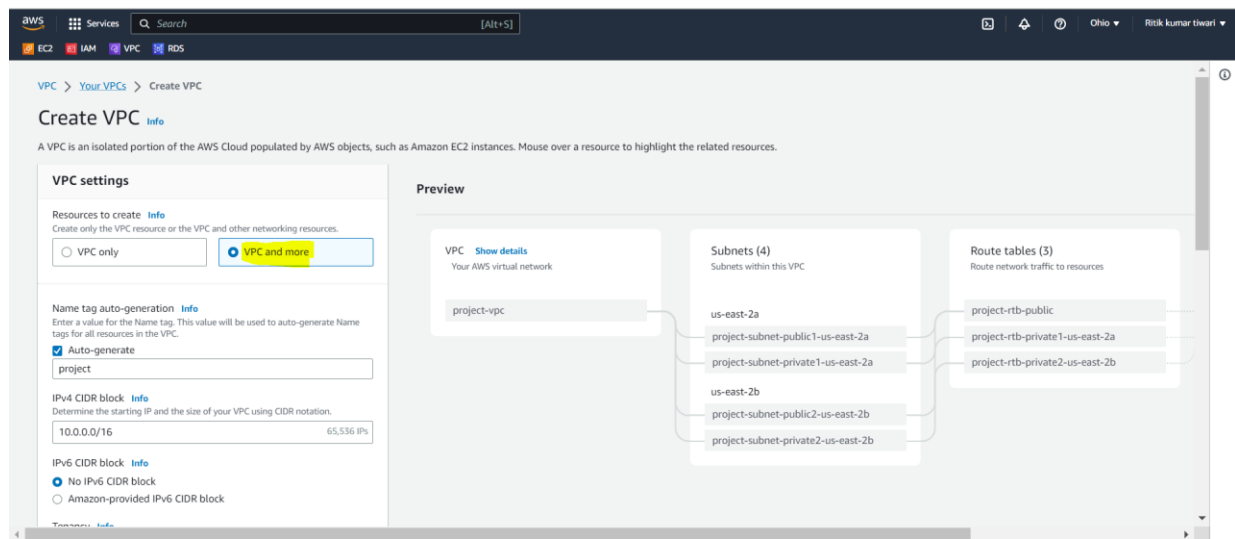
First Go to VPC and Create VPC:





Go with VPC and More because AWS will provide you default resource, which is already configured, we don't need to configure lots of things.

Like: VPC, Subnets for both the regions as a (public & Private) and route tables etc.



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
Demo-vpc

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

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

Demo-vpc-vpc

Subnets (4)
Subnets within this VPC

- us-east-2a
 - Demo-vpc-subnet-public1-us-east-2a
 - Demo-vpc-subnet-private1-us-east-2a
- us-east-2b
 - Demo-vpc-subnet-public2-us-east-2b
 - Demo-vpc-subnet-private2-us-east-2b

Route tables (3)
Route network traffic to resources

- Demo-vpc-rtb-public
- Demo-vpc-rtb-private1-us-east-2a
- Demo-vpc-rtb-private2-us-east-2b

You can modify IPv4 CIDR block according to your requirement.

Number of Availability Zones (AZs) [Info](#)
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1 2 3

► Customize AZs

Number of public subnets [Info](#)
The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0 2

Number of private subnets [Info](#)
The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0 2 4

► Customize subnets CIDR blocks

NAT gateways (\$) [Info](#)
Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway.

None In 1 AZ 1 per AZ

VPC endpoints [Info](#)
Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

None S3 Gateway

DNS options [Info](#)

☒ Enable DNS hostnames

☒ Enable DNS resolution

► Additional tags

Cancel Create VPC

Create VPC workflow

Associate route table

62%

Details

- ✓ Create VPC: [vpc-0563a71b517785ece](#)
- ✓ Enable DNS hostnames
- ✓ Enable DNS resolution
- ✓ Verifying VPC creation: [vpc-0563a71b517785ece](#)
- ✓ Create S3 endpoint: [vpce-03621cc19ea52a8c2](#)
- ✓ Create subnet: [subnet-0d77288f56498fdf5](#)
- ✓ Create subnet: [subnet-093d4300763ea893c](#)
- ✓ Create subnet: [subnet-0218e30802bad2081](#)
- ✓ Create subnet: [subnet-084c7d287b58eae54](#)
- ✓ Create internet gateway: [igw-0c7d949645c5caf07](#)
- ✓ Attach internet gateway to the VPC
- ✓ Create route table: [rtb-0e87fb2efb75e76ae](#)
- ✓ Create route
- ⚙ Associate route table
- ⌚ Associate route table
- ⌚ Create route table
- ⌚ Associate route table
- ⌚ Create route table
- ⌚ Associate route table

EC2 IAM VPC RDS

VPC > Your VPCs > Create VPC > Create VPC resources

Create VPC workflow

✓ Success

Details

- ✓ Create VPC: [vpc-0563a71b517785ece](#)
- ✓ Enable DNS hostnames
- ✓ Enable DNS resolution
- ✓ Verifying VPC creation: [vpc-0563a71b517785ece](#)
- ✓ Create S3 endpoint: [vpce-03621cc19ea52a8c2](#)

Click on **View VPC**

Wait for some time it will create and then you can see.

Your VPCs (1/2) Info

Find resources by attribute or tag



Actions

Create VPC

< 1 > ⚙

	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	M...
✓	Demo-vpc-vpc	vpc-0563a71b517785ece	Available	10.0.0.0/16	-	dopt-0e344741cc021a3...	rtl

Now we will create EC2 instance where we are going to demonstrate security group and NACL:

Go to instance

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name: [Add additional tags](#)

Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

Quick Start

Amazon Linux macOS **Ubuntu** Windows Red Hat SUSE Linux

Summary

Number of instances [Info](#): 1

Software Image (AMI): Canonical, Ubuntu, 22.04 LTS, ...[read more](#)
ami-024e6efaf93d85776

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in ...)

[Cancel](#) [Launch instance](#) [Review commands](#)

Quick Start

Amazon Linux macOS **Ubuntu** Windows Red Hat SUSE Linux

[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type [Free tier eligible](#)

ami-024e6efaf93d85776 (64-bit (x86)) / ami-08fdd91d87f63bb09 (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2023-05-16

Architecture **AMI ID**

64-bit (x86) ami-024e6efaf93d85776 [Verified provider](#)

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...[read more](#)
ami-024e6efaf93d85776

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in ...)

[Cancel](#) [Launch instance](#)

▼ Instance type
Info

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux pricing: 0.0116 USD per Hour
On-Demand SUSE pricing: 0.0116 USD per Hour
On-Demand Windows pricing: 0.0162 USD per Hour
On-Demand RHEL pricing: 0.0716 USD per Hour

☒ All generations

[Compare instance types](#)

▼ Key pair (login)
Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

my updated key

▼ Network settings
Info

You can create new key pair or existing one:

Click on EDIT:

Please don't go with default VPC, select your own VPC as we created previous **Demo VPC**

▼ Network settings
Info

Network
Info

vpc-0f4b4e172b5686fa5

Subnet
Info

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

We'll create a new security group called 'launch-wizard-12' with the following rules:

☒ Allow SSH traffic from

Helps you connect to your instance

Anywhere
0.0.0.0/0

☐ Allow HTTPS traffic from the internet

To set up an endpoint, for example when creating a web server

☐ Allow HTTP traffic from the internet

To set up an endpoint, for example when creating a web server

▼ Network settings [Info](#)

VPC - *required* [Info](#)

vpc-0563a71b517785ece (Demo-vpc-vpc) ↻
10.0.0.0/16

Subnet [Info](#)

subnet-0d77288f56498fdf5 **Demo-vpc-subnet-public1-us-east-2a** ↻ [Create new subnet](#)
VPC: vpc-0563a71b517785ece Owner: 703252462768
Availability Zone: us-east-2a IP addresses available: 4091 CIDR: 10.0.0.0/20

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

Security group name - *required*

launch-wizard-12


This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&:{}!\$*

Description - *required* [Info](#)

launch-wizard-12 created 2023-07-16T09:05:35.468Z

Rest of things should be default and click on Launch instance.

[EC2](#) > [Instances](#) > **Launch an instance**



Success
Successfully initiated launch of instance (i-09b1bddbd038f9f7e)

▶ **Launch log**

Now we install Python, and we will deploy and run that application on EC2 Port No. 8000, it will be block by default, but we need to enable that. Let see.

Instances (1) [Info](#)

↻ [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
<input type="checkbox"/>	Demo	i-09b1bddbd038f9f7e	Running	t2.micro	2/2 checks passed	No alarms	us-east-2a	ec2-18-191-212-194.us...	18.191.212.194	-

sudo apt update

python3 (check python is installed or not)

```
ubuntu@ip-10-0-14-242:~$ python3
Python 3.10.6 (main, Mar 10 2023, 10:55:28) [GCC 11.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

Ctrl+D go main server:

Pyhon3 -m http.server 8000

It is running on this server...

```
Try: sudo apt install <deb name>
ubuntu@ip-10-0-14-242:~$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

If we want to access this application through instance Public IP address, it will not show the page...

i-09b1bddbd038f9f7e (Demo)

PublicIPs: 18.191.212.194 PrivateIPs: 10.0.14.242

Copy the public ip : <http://18.191.212.194:8000/>



This site can't be reached

18.191.212.194 took too long to respond.

Try:

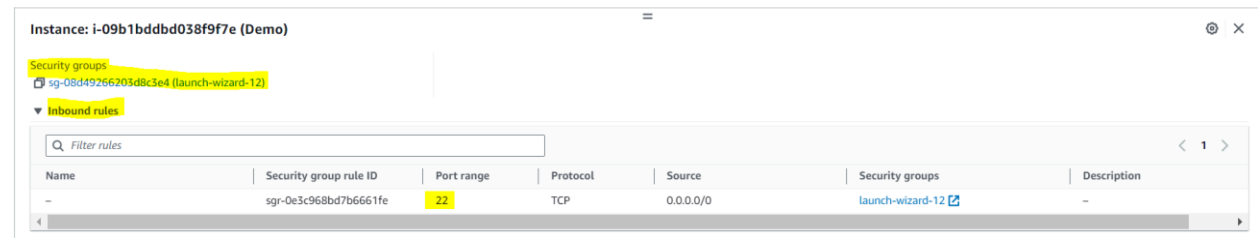
- Checking the connection
- [Checking the proxy and the firewall](#)
- [Running Windows Network Diagnostics](#)

ERR_CONNECTION_TIMED_OUT

Reload

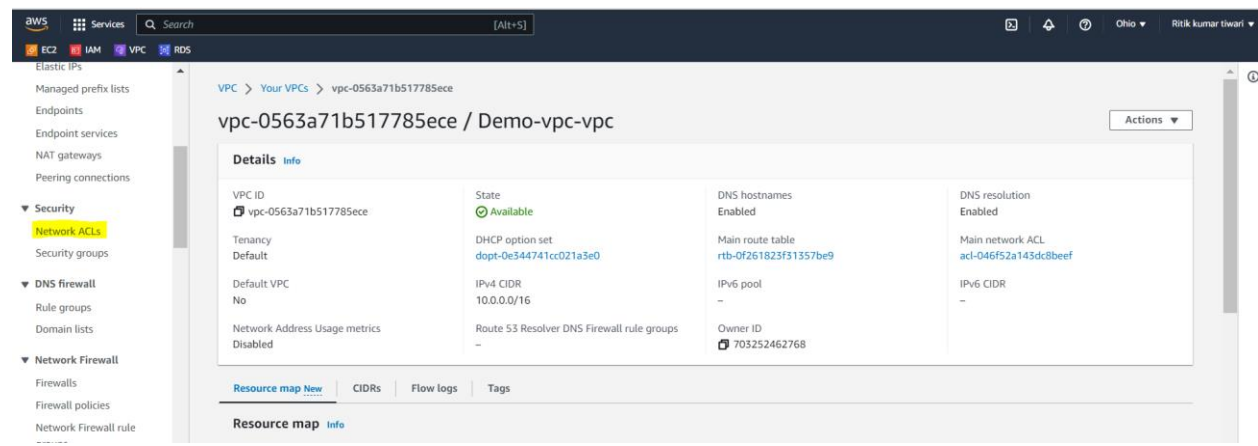
It will throw site can't find.

Go to instance > security > security group > inbound rule port 22> aws by default allow.. there is no 8000 port.

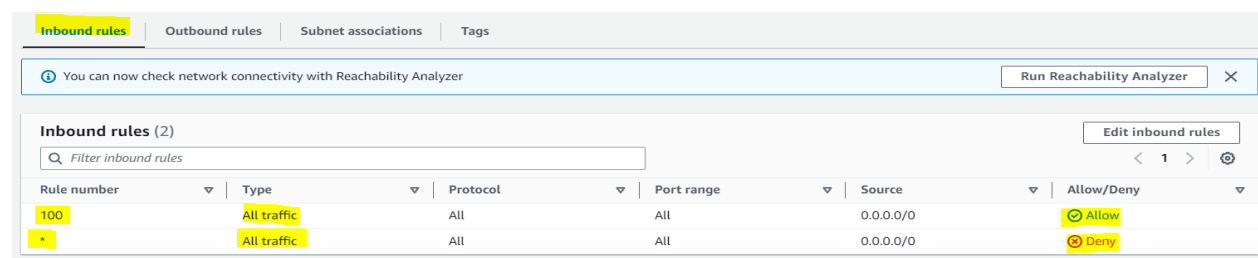
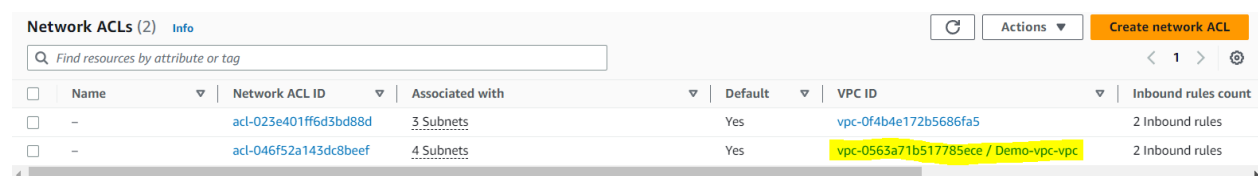


Now we will investigate NACL concept:

Go-to VPC > click on your newly created VPC > click on Network CALs



Click on Network ACL ID:

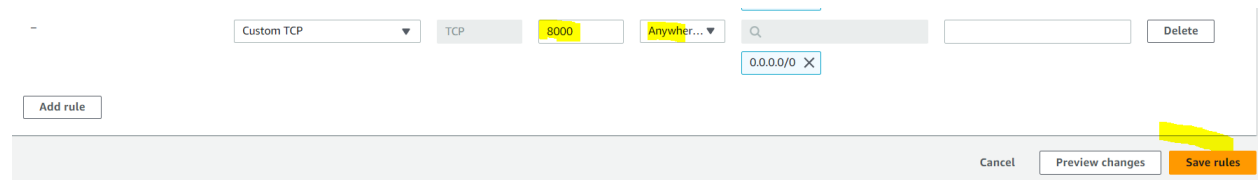
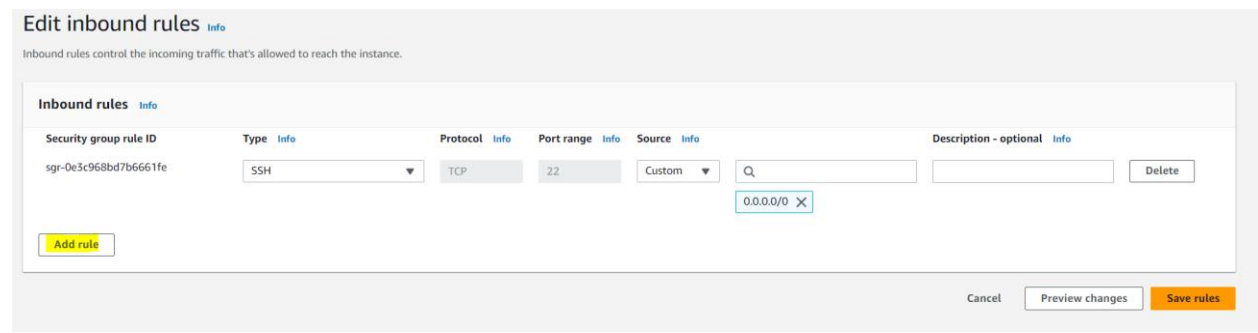
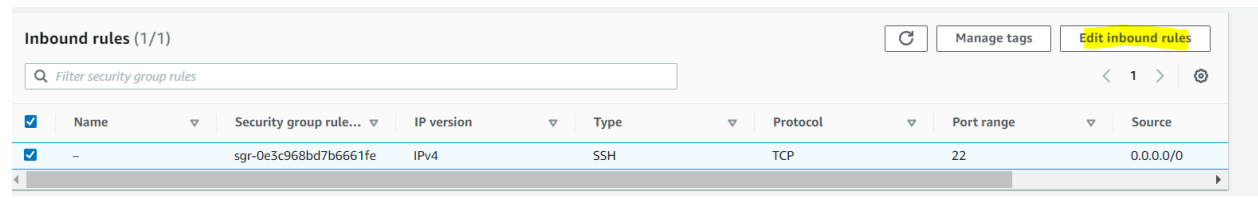
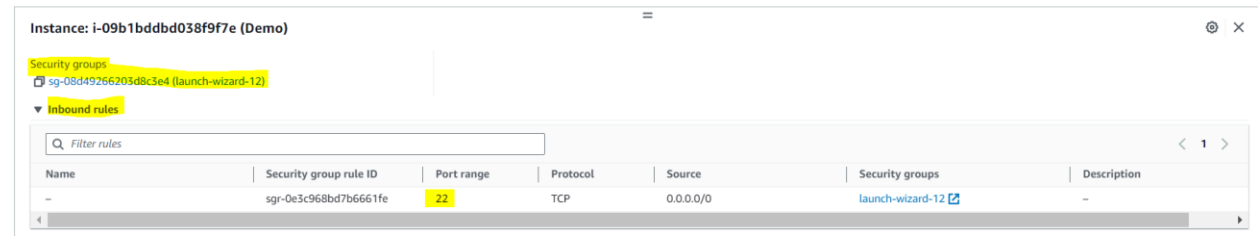


There is rule 100, it will check if requirement meet it will pass otherwise it will fail,

So as of now... we need to edit the inbound rule in security group.

Go to instance > security > security group > inbound rule port 22> aws by default allow. there is not 8000 port.

Now we need to allow port no. 8000



Copy the public ip and paste it on browser: <http://18.191.212.194:8000/>

Now paste the URL, we will see simple http sever, where all the files are present in this folders this is the output:

Directory listing for /

- [.bash_logout](#)
- [.bashrc](#)
- [.cache/](#)
- [.profile](#)
- [.python_history](#)
- [.ssh/](#)
- [sudo_as_admin_successful](#)

```
ubuntu@ip-10-0-14-242:~$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
49.36.169.138 - - [16/Jul/2023 09:54:34] "GET / HTTP/1.1" 200 -
49.36.169.138 - - [16/Jul/2023 09:54:41] "GET / HTTP/1.1" 200 -
```

If you will refresh the web page, then you will see the response 200.

  Strengthening Security with NACLs: Blocking Port 8000 to Enforce Strict Rules!  

As a DevOps engineer. Suppose in your organization has very strict rule that we cannot allow permission to enable the port no. 8000, then I will block the port 8000 in NACL on subnet level

VPC > Network ACLs > acl-023e401ff6d3bd88d > Edit inbound rules

Edit inbound rules [Info](#)
Inbound rules control the incoming traffic that's allowed to reach the VPC.

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

Add new rule Sort by rule number

Cancel Preview changes Save changes

Then request will not go to the application team, or that application will not open.

Inbound rules							
You can now check network connectivity with Reachability Analyzer							
Run Reachability Analyzer							
Inbound rules (2)							
Filter inbound rules							
Edit inbound rules							
< 1 > ⚙							
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		



This site can't be reached

18.191.212.194 refused to connect.

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)

ERR_CONNECTION_REFUSED

Reload

So, who has permission of the NACL, they can block the all the IP-addresses over all the subnet level.

Note:

We have understood the topic of NACL and security group, with respect to allowing and blocking the access.

Follow for more on LinkedIn: <https://www.linkedin.com/in/ritikktiware/>