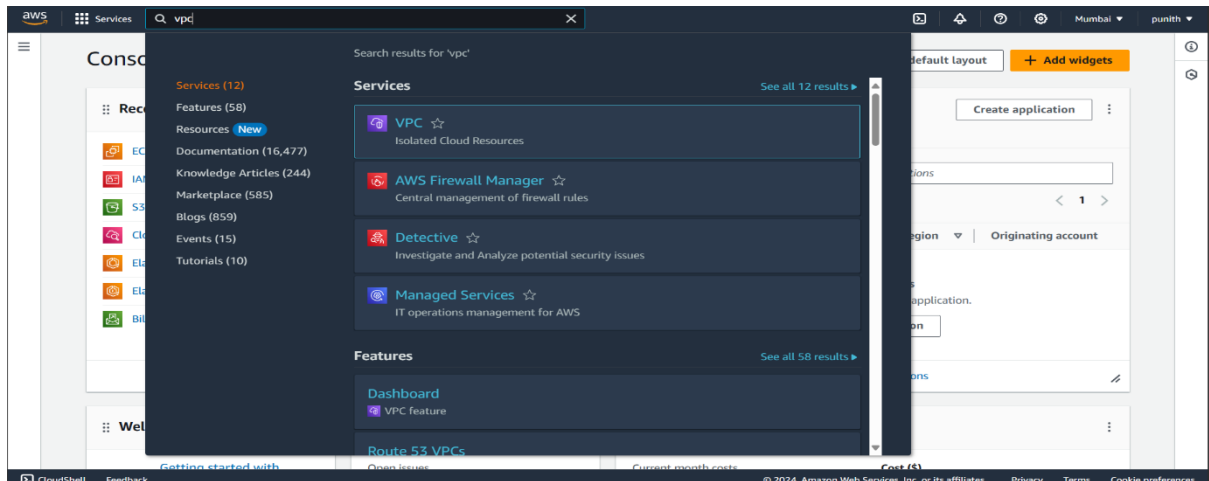


# VPC(Virtual Private Cloud)

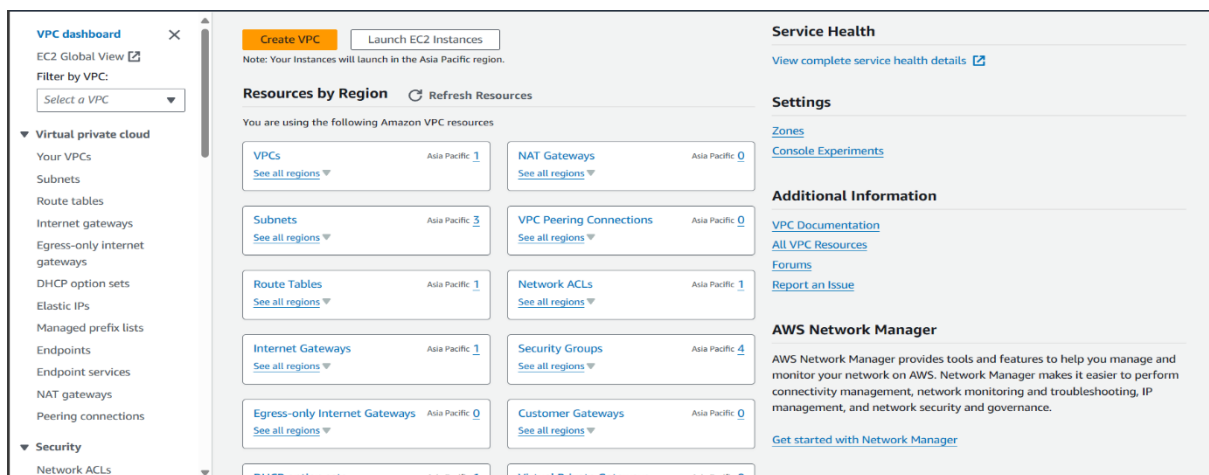
- VPC stands for Virtual Private Cloud and it is a private cloud that can be created inside a public cloud. It can be used in our own data centres and availability zones. By default, AWS provides a default VPC for every user.
- VPC contains components like IP Addresses, Subnets, Route-Table, Security Groups, NACL, Internet Gateways, NAT etc..  
Each component have been explained in detail below:
- IP Address: IP Address allows users to connect to internet or server. AWS provides IPV4 and IPV6 addresses that are CIDR.
- Subnet: The subnets defines the range of ip address of each ec2. Here, We have public subnets and private subnets.
- Route-Table: Route Tables helps to direct the network traffic from subnets, gateways.
- Security Groups: These security groups helps to control the traffic at an ec2 from inbound and outbound rules.
- NACL: NACL stands for Network Access Control List and they allows or denies specific traffic at the subnet level.
- NAT: NAT stands for Network Address Translation and NAT helps to connect and access the resources and services like ec2 from outside the VPC with private subnet.
- Internet Gateways: Allows communication between the VPC and Internet.

- Now, We see how to create a custom VPC and attach to EC2 and deploy the EC2 on server with photos attached below:

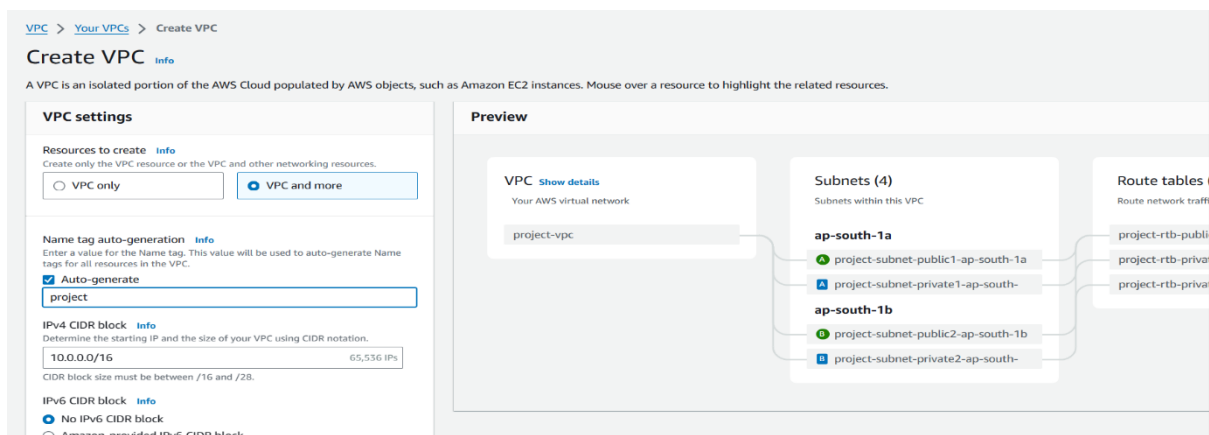
Login to AWS console and search for VPC.



This is how VPC dashboard looks like. Choose create VPC.



Choose VPC and more and name the VPC.



Select the no.of availability zones,Public and Private subnets to be created.

**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**

Choose the default settings and enable the DNS options.Choose create VPC.

**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

One by one, the VPC configuration gets created. Choose view VPC.

Success

Details

✔ Create VPC: [vpc-08ef6002ef26aa463](#)

✔ Enable DNS hostnames

✔ Enable DNS resolution

✔ Verifying VPC creation: [vpc-08ef6002ef26aa463](#)

✔ Create S3 endpoint: [vpce-0a58412414f1913e4](#)

✔ Create subnet: [subnet-01a6707bd3e9baecf](#)

✔ Create subnet: [subnet-0bdc2afa33070338c](#)

✔ Create subnet: [subnet-0b34ef6759e54c872](#)

✔ Create subnet: [subnet-079a55192fc17f944](#)

✔ Create internet gateway: [igw-02c7076ce6a853ff7](#)

✔ Attach internet gateway to the VPC

✔ Create route table: [rtb-0999d8d4c1c9963ff](#)

✔ Create route

✔ Associate route table

✔ Associate route table

✔ Create route table: [rtb-0fe68941aa9aced97](#)

✔ Associate route table

✔ Create route table: [rtb-0246f7341bfcee4d5](#)

✔ Associate route table

✔ Verifying route table creation

✔ Associate S3 endpoint with private subnet route tables: [vpce-0a58412414f1913e4](#)

View VPC

You can see the overview of the VPC created.

VPC > Your VPCs > vpc-08ef6002ef26aa463

vpc-08ef6002ef26aa463 / project-vpc

Actions

Details

VPC ID vpc-08ef6002ef26aa463	State ✔ Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-04e8bd2efcf93b01	Main route table <a href="#">rtb-0fed3a08d898d36ef</a>	Main network ACL <a href="#">acl-07b652000fc8dbc7d</a>
Default VPC No	IPv4 CIDR 10.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 211125559768	

Resource map

CIDRs | Flow logs | Tags | Integrations

Resource map

VPC  
Show details  
Your AWS virtual network

Subnets (4)  
Subnets within this VPC

Route tables (4)  
Route network traffic to resources

Comeback to EC2 and Launch an instance.

EC2

>

Instances

>

Launch an 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

demo

Add additional tags

Choose ubuntu and it's version.

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

Q

Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE Li

SUSE

Q

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-007020fd9c84e18c7 (64-bit (x86)) / ami-09c443d9277298026 (64-bit (Arm))

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

Choose instance type and the key-pair.

Instance type

Info | Get advice

Instance type

t2.micro

Free tier eligible

Family: t2    1 vCPU    1 GiB Memory    Current generation: true

On-Demand Linux base pricing: 0.0124 USD per Hour

On-Demand Windows base pricing: 0.017 USD per Hour

On-Demand RHEL base pricing: 0.0724 USD per Hour

On-Demand SUSE base pricing: 0.0124 USD per Hour

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

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

instance-key-pair

Create new key pair

Here, We have choose our VPC created,public subnet and enable auto-assign public IP. Choose to create a new security group and name it.

▼ Network settings

Info

VPC - required

Info

vpc-08ef6002ef26aa463 (project-vpc)

10.0.0.0/16

▼

↻

Subnet

Info

subnet-01a6707bd3e9baecf

project-subnet-public1-ap-south-1a

▼

↻

Create new subnet

↗

VPC: vpc-08ef6002ef26aa463

Owner: 211125559768

Availability Zone: ap-south-1a

IP addresses available: 4091

CIDR: 10.0.0.0/20

Auto-assign public IP

Info

Enable

▼

Additional charges apply

when outside of free tier allowance

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

vpc-ec2-connect

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-4 created 2024-04-20T11:06:40.020Z

Keep it default and we will see in deep in upcoming images.

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

Remove

Type

Info

ssh

▼

Protocol

Info

TCP

Port range

Info

22

Source type

Info

Anywhere

▼

Source

Info

Q Add CIDR, prefix list or security

0.0.0.0/0

×

Description - optional

Info

e.g. SSH for admin desktop

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

×

Add security group rule

► Advanced network configuration

Choose the storage size and launch instance.

▼ Configure storage Info

Advanced

1x 10 GiB gp2 Root volume (Not encrypted)

Add new volume

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

Click refresh to view backup information

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems

Edit

Software Image (AMI)  
Canonical, Ubuntu, 22.04 LTS, ...read more  
ami-007020fd9c84e18c7

Virtual server type (instance type)  
t2.micro

Firewall (security group)  
New security group

Storage (volumes)  
1 volume(s) - 10 GiB

Cancel

Launch instance

Review commands

Here, We can see the VPC that we have attached to the instance.

Instance summary for i-0bcb77b44717c9c47 (demo) Info

Updated less than a minute ago

Connect Instance state Actions

Instance ID  
i-0bcb77b44717c9c47 (demo)

IPV6 address  
-

Hostname type  
IP name: ip-10-0-13-165.ap-south-1.compute.internal

Answer private resource DNS name  
-

Auto-assigned IP address  
65.0.26.152 [Public IP]

IAM Role  
-

IMDSv2  
Required

Public IPv4 address  
65.0.26.152 open address

Instance state  
Running

Private IP DNS name (IPv4 only)  
ip-10-0-13-165.ap-south-1.compute.internal

Instance type  
t2.micro

VPC ID  
vpc-08ef6002ef26aa463 (project-vpc)

Subnet ID  
subnet-01a6707bd3e9baecf (project-subnet-public1-ap-south-1a)

Private IPv4 addresses  
10.0.13.165

Public IPv4 DNS  
ec2-65-0-26-152.ap-south-1.compute.amazonaws.com open address

Elastic IP addresses  
-

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

Auto Scaling Group name  
-

Connect the instance to browser.

EC2 > Instances > i-0bcb77b44717c9c47 > Connect to instance

Connect to instance Info

Connect to your instance i-0bcb77b44717c9c47 (demo) using any of these options

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID  
i-0bcb77b44717c9c47 (demo)

Connection Type  

Connect using EC2 Instance Connect  
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.

Connect using EC2 Instance Connect Endpoint  
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Public IP address  
65.0.26.152

Username  
Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ubuntu.  
ubuntu

Go to root and update the packages.

```
ubuntu@ip-10-0-13-165:~$ sudo su -  
root@ip-10-0-13-165:~# apt update
```

Install apache2 http server on instance. It helps the instance to connect on http server using port 80.

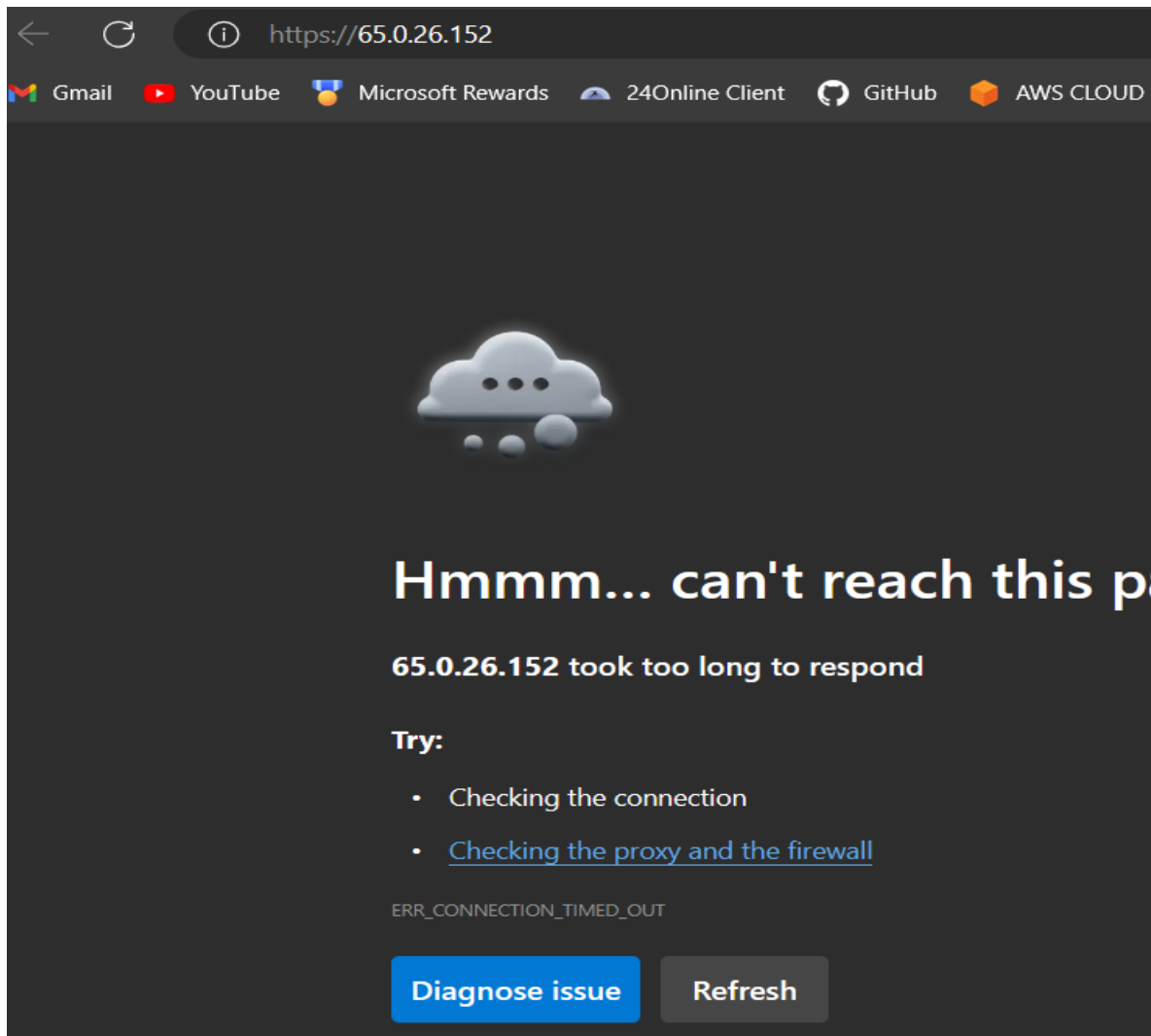
```
root@ip-10-0-13-165:~# apt install apache2
```

Check the status of the apache2 server.

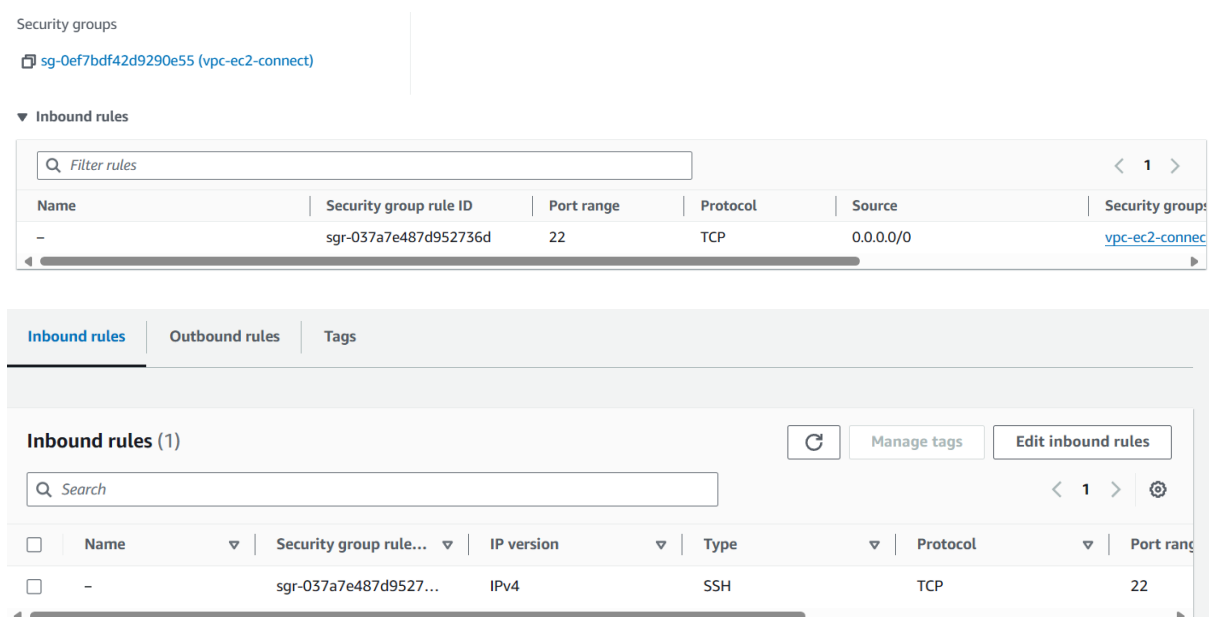
```
root@ip-10-0-13-165:~# systemctl status apache2  
● apache2.service - The Apache HTTP Server  
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)  
   Active: active (running) since Sat 2024-04-20 11:17:11 UTC; 17s ago  
     Docs: https://httpd.apache.org/docs/2.4/  
  Main PID: 2652 (apache2)  
    Tasks: 55 (limit: 1121)  
   Memory: 4.9M  
      CPU: 33ms  
   CGroup: /system.slice/apache2.service  
           └─2652 /usr/sbin/apache2 -k start  
             └─2654 /usr/sbin/apache2 -k start  
               └─2655 /usr/sbin/apache2 -k start  
  
Apr 20 11:17:10 ip-10-0-13-165 systemd[1]: Starting The Apache HTTP Server...  
Apr 20 11:17:11 ip-10-0-13-165 systemd[1]: Started The Apache HTTP Server.  
root@ip-10-0-13-165:~#
```

Go to the browser and check if the http server is working successfully. It won't work because we haven't configured the http and the port in security group in inbound rules.

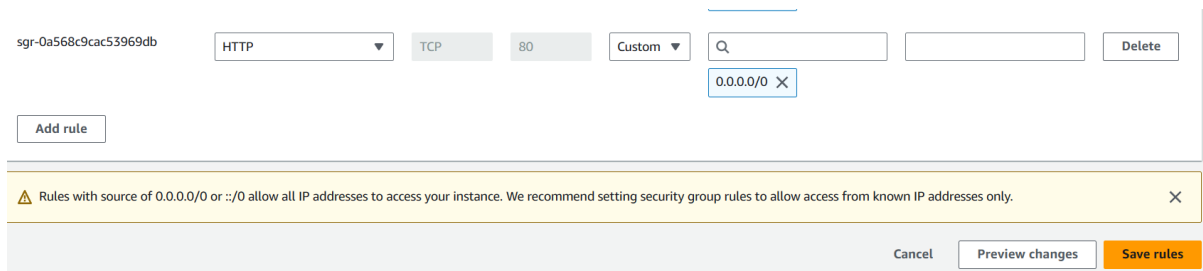




Comeback to instance and go to security groups. Choose the security group. Click on edit inbound rules to add the protocol and port.

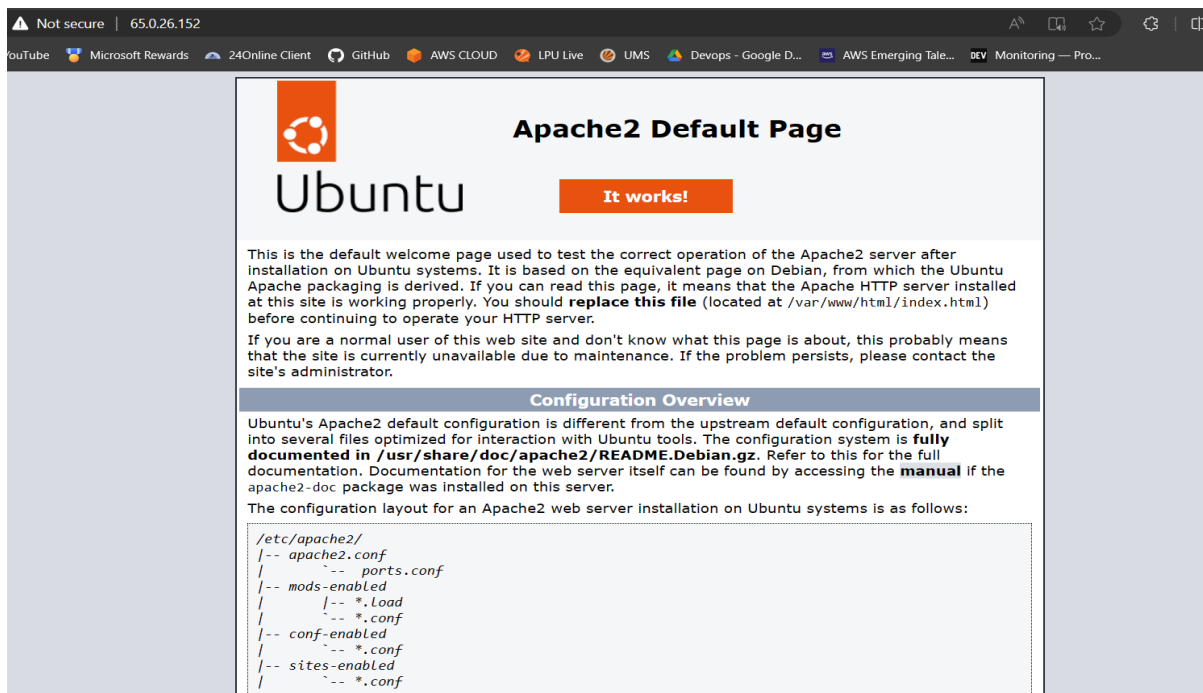


Add HTTP protocol and save the rules.

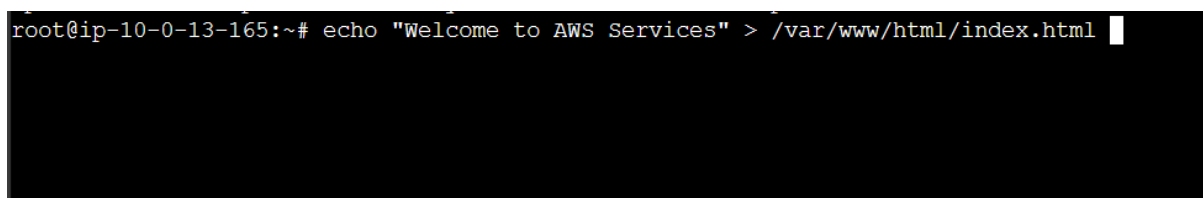


The screenshot shows the AWS Security Groups console. At the top, there's a rule configuration bar with the ID 'sgr-0a568c9cac53969db'. The protocol is set to 'HTTP', action to 'Allow', and port range to '80'. The source is set to 'Custom' with a search icon and a dropdown showing '0.0.0.0/0'. There's a 'Delete' button. Below this is an 'Add rule' button. A yellow warning banner states: '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.' At the bottom are 'Cancel', 'Preview changes', and 'Save rules' buttons.

Enter the IP of instance again and we can see the http server running.

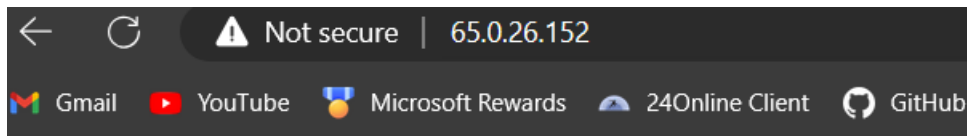


Here, We can customize the server settings and enter the command shown below.



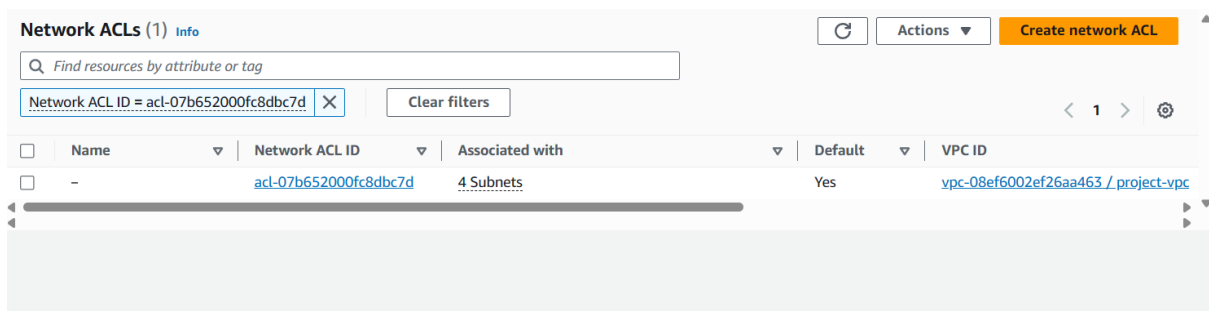
```
root@ip-10-0-13-165:~# echo "Welcome to AWS Services" > /var/www/html/index.html
```

This command enters the text into the index.html file and gets displayed when we again refresh the http page.

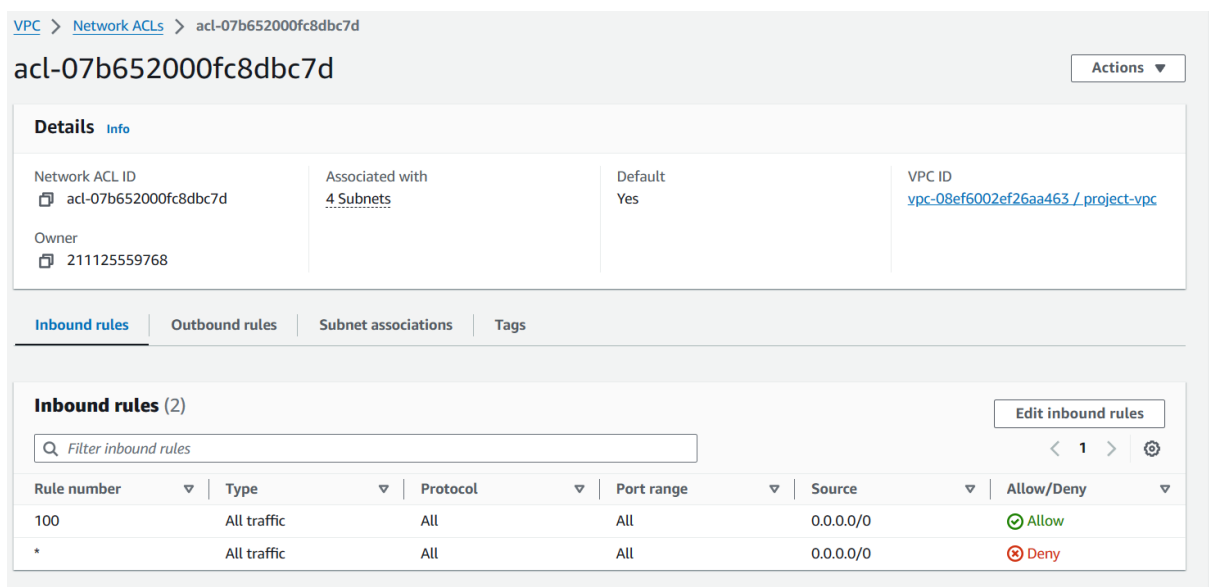


Welcome to AWS Services

Now, We see how NACL can be used and the main difference between SG and NACL. Choose the NACL ID that is already created for the VPC.



We can see, the inbound rules are in an order i.e the NACL verifies the first rule that is mentioned in order and allows or denies traffic accordingly.



Choose edit inbound rules. Add new rule and give rule number and change the configuration accordingly mentioned below. Save the changes.

**Edit inbound rules** [Info](#)

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

Rule number <a href="#">Info</a>	Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Allow/Deny <a href="#">Info</a>	
100	All traffic ▼	All ▼	All	0.0.0.0/0	Deny ▼	<button>Remove</button>
250	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

We can see, the rule number 100 has the priority and it is denied to allow the traffic. Now, open the instance ip on new page and let's see what happens.

Inbound rules

Outbound rules

Subnet associations

Tags

Inbound rules (3)

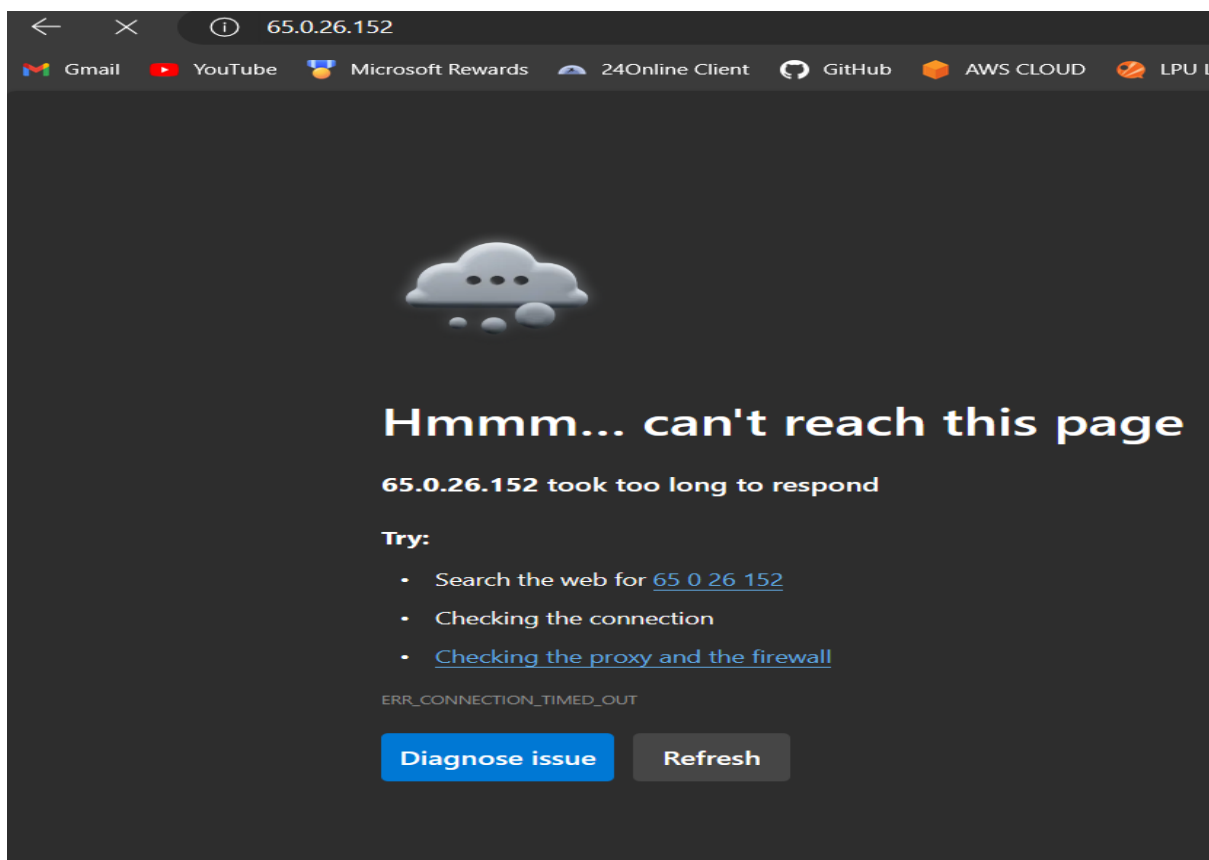
Edit inbound rules

Q Filter inbound rules

< 1 >

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

We can see that it denied the access to the http server.



A small discussion on subnets i.e whenever a VPC is created, both public and private subnets get created for VPC in the availability zones that currently you belong to and a default route table also gets created.

Subnets (1/7) Info

Find resources by attribute or tag

Actions

Create subnet

	Name	Subnet ID	State	VPC	IPv4 CIDR
<input checked="" type="checkbox"/>	project-subnet-public1-ap-south-1a	<a href="#">subnet-01a6707bd3e9baecf</a>	Available	<a href="#">vpc-08ef6002ef26aa463</a>   <a href="#">proj...</a>	10.0.0.0/20
<input type="checkbox"/>	project-subnet-public2-ap-south-1b	<a href="#">subnet-0bdc2afa33070338c</a>	Available	<a href="#">vpc-08ef6002ef26aa463</a>   <a href="#">proj...</a>	10.0.16.0/20

subnet-01a6707bd3e9baecf / project-subnet-public1-ap-south-1a

Details | Flow logs | Route table | Network ACL | CIDR reservations | Sharing | Tags

Details

Subnet ID

subnet-01a6707bd3e9baecf

Available IPv4 addresses

4090

Network border group

ap-south-1

Default subnet

No

Subnet ARN

arn:aws:ec2:ap-south-1:211125559768:subnet/subnet-01a6707bd3e9baecf

IPv6 CIDR

–

VPC

[vpc-08ef6002ef26aa463](#) | [project-vpc](#)

Auto-assign public IPv4 address

No

State

Available

Availability Zone

ap-south-1a

Route table

[rtb-0999d8d4c1c9963ff](#) | [project-rtb-public](#)

Auto-assign IPv6 address

No

IPv4 CIDR

10.0.0.0/20

Availability Zone ID

aps1-az1

Network ACL

[acl-07b652000fc8dbc7d](#)

Auto-assign customer-owned IPv4 address

No