CLOUD FORMATION VPC TASK

Problem Statement: You work for XYZ Corporation. Your team is asked to deploy similar architecture multiple times for testing, development, and production purposes. Implement CloudFormation for the tasks assigned to you below.

Tasks To Be Performed:

1. Create a template with 1 VPC and 1 public subnet.
2. Launch an Amazon Linux EC2 instance in the public subnet and tag the instance as "CFinstance

First create a template using this code save as yaml file

```
Description:  This template deploys a VPC, with a pair of public and private subnets spread
  across two Availability Zones. It deploys an internet gateway, with a default
  route on the public subnets. It deploys a pair of NAT gateways (one in each AZ),
  and default routes for them in the private subnets.

Parameters:
  EnvironmentName:
    Description: An environment name that is prefixed to resource names
    Type: String

  VpcCIDR:
    Description: Please enter the IP range (CIDR notation) for this VPC
    Type: String
    Default: 10.192.0.0/16

  PublicSubnet1CIDR:
    Description: Please enter the IP range (CIDR notation) for the public subnet in the first
Availability Zone
    Type: String
    Default: 10.192.10.0/24

  PublicSubnet2CIDR:
    Description: Please enter the IP range (CIDR notation) for the public subnet in the second
Availability Zone
    Type: String
    Default: 10.192.11.0/24

  PrivateSubnet1CIDR:
    Description: Please enter the IP range (CIDR notation) for the private subnet in the first
Availability Zone
    Type: String
    Default: 10.192.20.0/24
```

```
  PrivateSubnet2CIDR:
    Description: Please enter the IP range (CIDR notation) for the private subnet in the second
Availability Zone
    Type: String
    Default: 10.192.21.0/24

Resources:
  VPC:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: !Ref VpcCIDR
      EnableDnsSupport: true
      EnableDnsHostnames: true
      Tags:
        - Key: Name
          Value: !Ref EnvironmentName

  InternetGateway:
    Type: AWS::EC2::InternetGateway
    Properties:
      Tags:
        - Key: Name
          Value: !Ref EnvironmentName

  InternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      InternetGatewayId: !Ref InternetGateway
      VpcId: !Ref VPC

  PublicSubnet1:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPC
      AvailabilityZone: !Select [ 0, !GetAZs '' ]
      CidrBlock: !Ref PublicSubnet1CIDR
      MapPublicIpOnLaunch: true
      Tags:
        - Key: Name
          Value: !Sub ${EnvironmentName} Public Subnet (AZ1)

  PublicSubnet2:
    Type: AWS::EC2::Subnet
```

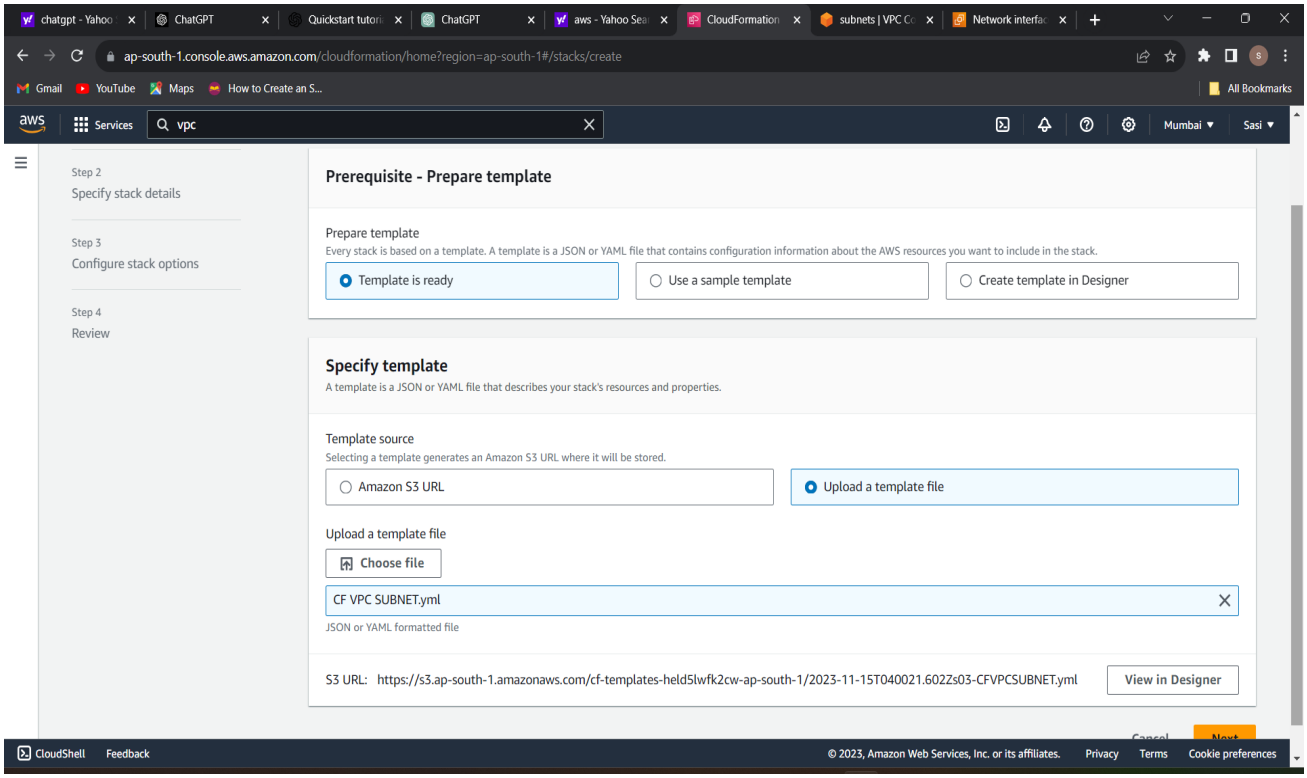
```
  Properties:
    VpcId: !Ref VPC
    AvailabilityZone: !Select [ 1, !GetAZs  '' ]
    CidrBlock: !Ref PublicSubnet2CIDR
    MapPublicIpOnLaunch: true
    Tags:
      - Key: Name
        Value: !Sub ${EnvironmentName} Public Subnet (AZ2)

PrivateSubnet1:
  Type: AWS::EC2::Subnet
  Properties:
    VpcId: !Ref VPC
    AvailabilityZone: !Select [ 0, !GetAZs  '' ]
    CidrBlock: !Ref PrivateSubnet1CIDR
    MapPublicIpOnLaunch: false
    Tags:
      - Key: Name
        Value: !Sub ${EnvironmentName} Private Subnet (AZ1)

PrivateSubnet2:
  Type: AWS::EC2::Subnet
  Properties:
    VpcId: !Ref VPC
    AvailabilityZone: !Select [ 1, !GetAZs  '' ]
    CidrBlock: !Ref PrivateSubnet2CIDR
    MapPublicIpOnLaunch: false
    Tags:
      - Key: Name
        Value: !Sub ${EnvironmentName} Private Subnet (AZ2)

NatGateway1EIP:
  Type: AWS::EC2::EIP
  DependsOn: InternetGatewayAttachment
  Properties:
    Domain: vpc

NatGateway2EIP:
  Type: AWS::EC2::EIP
  DependsOn: InternetGatewayAttachment
  Properties:
    Domain: vpc

NatGateway1:
```

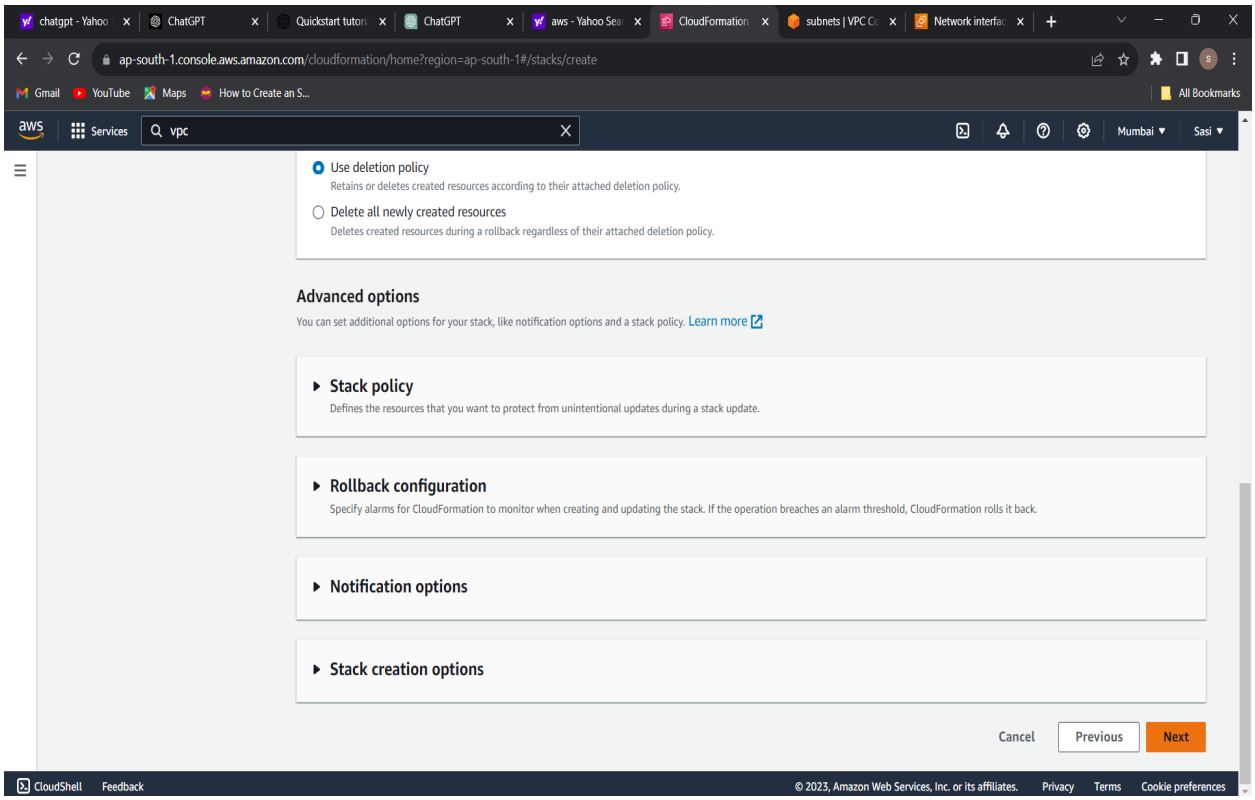
```
  Type: AWS::EC2::NatGateway
  Properties:
    AllocationId: !GetAtt NatGateway1EIP.AllocationId
    SubnetId: !Ref PublicSubnet1

NatGateway2:
  Type: AWS::EC2::NatGateway
  Properties:
    AllocationId: !GetAtt NatGateway2EIP.AllocationId
    SubnetId: !Ref PublicSubnet2

PublicRouteTable:
  Type: AWS::EC2::RouteTable
  Properties:
    VpcId: !Ref VPC
    Tags:
      - Key: Name
        Value: !Sub ${EnvironmentName} Public Routes

DefaultPublicRoute:
  Type: AWS::EC2::Route
  DependsOn: InternetGatewayAttachment
  Properties:
    RouteTableId: !Ref PublicRouteTable
    DestinationCidrBlock: 0.0.0.0/0
    GatewayId: !Ref InternetGateway

PublicSubnet1RouteTableAssociation:
  Type: AWS::EC2::SubnetRouteTableAssociation
  Properties:
    RouteTableId: !Ref PublicRouteTable
    SubnetId: !Ref PublicSubnet1

PublicSubnet2RouteTableAssociation:
  Type: AWS::EC2::SubnetRouteTableAssociation
  Properties:
    RouteTableId: !Ref PublicRouteTable
    SubnetId: !Ref PublicSubnet2


PrivateRouteTable1:
  Type: AWS::EC2::RouteTable
  Properties:
    VpcId: !Ref VPC
```

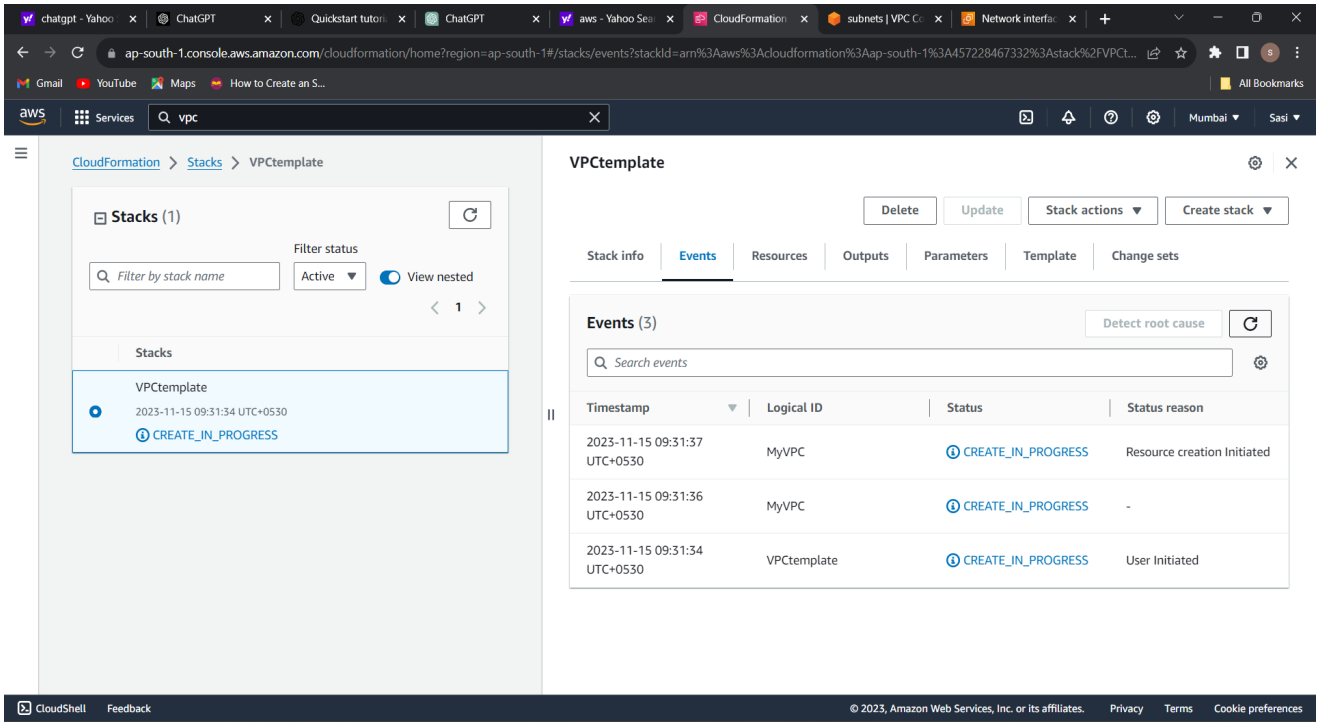
```
    Tags:
      - Key: Name
        Value: !Sub ${EnvironmentName} Private Routes (AZ1)

DefaultPrivateRoute1:
  Type: AWS::EC2::Route
  Properties:
    RouteTableId: !Ref PrivateRouteTable1
    DestinationCidrBlock: 0.0.0.0/0
    NatGatewayId: !Ref NatGateway1

PrivateSubnet1RouteTableAssociation:
  Type: AWS::EC2::SubnetRouteTableAssociation
  Properties:
    RouteTableId: !Ref PrivateRouteTable1
    SubnetId: !Ref PrivateSubnet1

PrivateRouteTable2:
  Type: AWS::EC2::RouteTable
  Properties:
    VpcId: !Ref VPC
    Tags:
      - Key: Name
        Value: !Sub ${EnvironmentName} Private Routes (AZ2)

DefaultPrivateRoute2:
  Type: AWS::EC2::Route
  Properties:
    RouteTableId: !Ref PrivateRouteTable2
    DestinationCidrBlock: 0.0.0.0/0
    NatGatewayId: !Ref NatGateway2

PrivateSubnet2RouteTableAssociation:
  Type: AWS::EC2::SubnetRouteTableAssociation
  Properties:
    RouteTableId: !Ref PrivateRouteTable2
    SubnetId: !Ref PrivateSubnet2

NoIngressSecurityGroup:
  Type: AWS::EC2::SecurityGroup
  Properties:
    GroupName: "no-ingress-sg"
    GroupDescription: "Security group with no ingress rule"
    VpcId: !Ref VPC
```

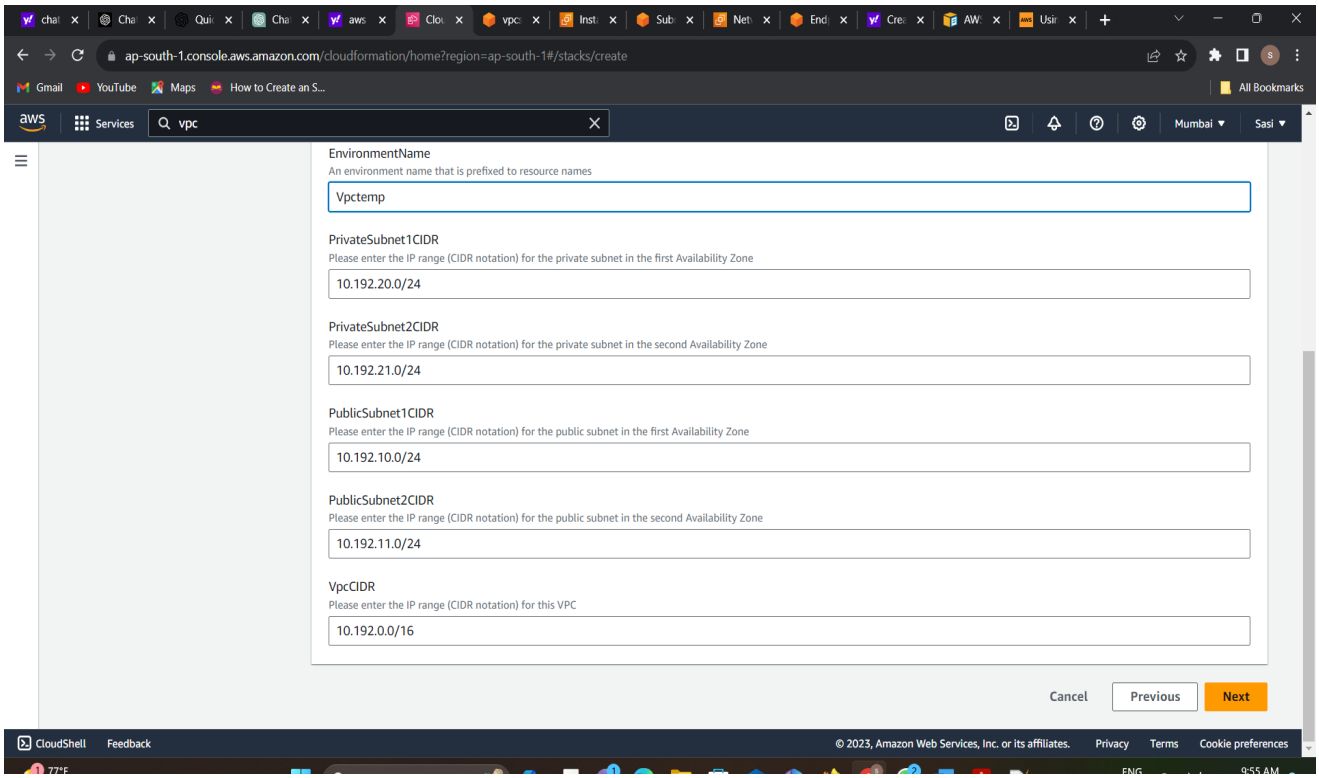
```
Outputs:
  VPC:
    Description: A reference to the created VPC
    Value: !Ref VPC

  PublicSubnets:
    Description: A list of the public subnets
    Value: !Join [ ",", [ !Ref PublicSubnet1, !Ref PublicSubnet2 ]]

  PrivateSubnets:
    Description: A list of the private subnets
    Value: !Join [ ",", [ !Ref PrivateSubnet1, !Ref PrivateSubnet2 ]]

  PublicSubnet1:
    Description: A reference to the public subnet in the 1st Availability Zone
    Value: !Ref PublicSubnet1

  PublicSubnet2:
    Description: A reference to the public subnet in the 2nd Availability Zone
    Value: !Ref PublicSubnet2

  PrivateSubnet1:
    Description: A reference to the private subnet in the 1st Availability Zone
    Value: !Ref PrivateSubnet1

  PrivateSubnet2:
    Description: A reference to the private subnet in the 2nd Availability Zone
    Value: !Ref PrivateSubnet2

  NoIngressSecurityGroup:
    Description: Security group with no ingress rule
    Value: !Ref NoIngressSecurityGroup
```

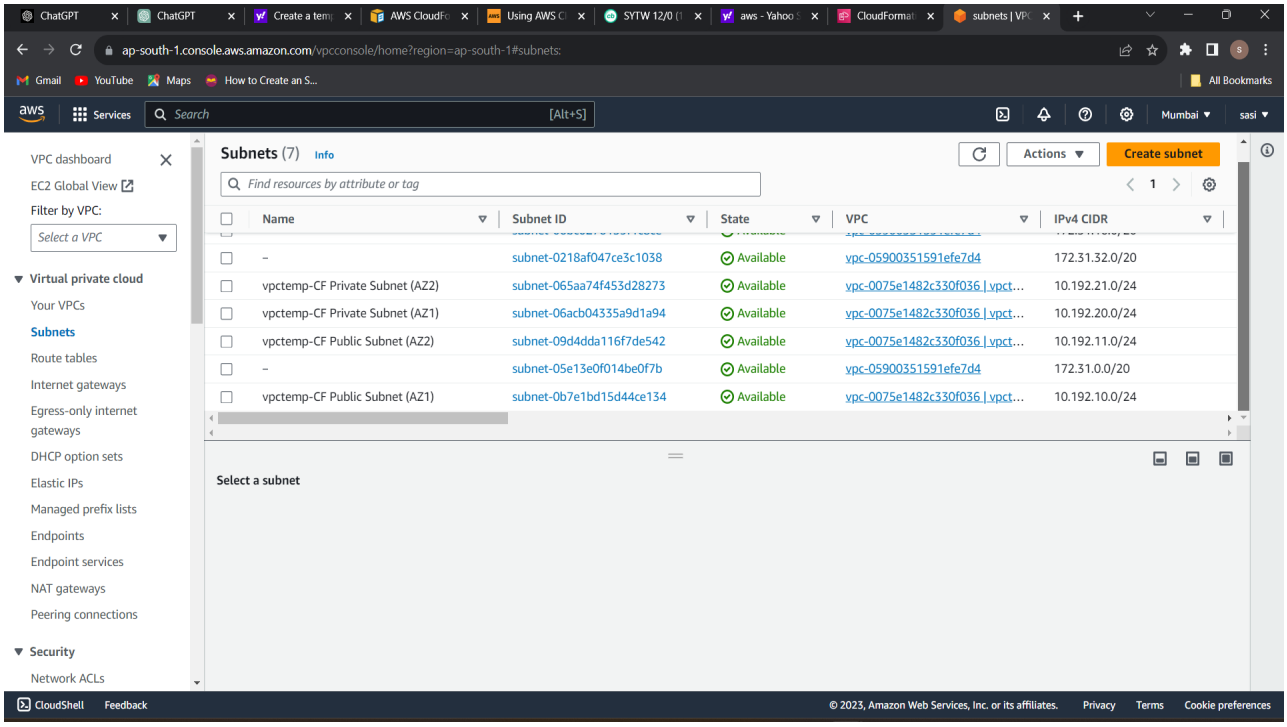
Now that our template file is ready to go, let's navigate back to the CloudFormation console. We previously had clicked the "Create stack" button, so you should see the screen below.

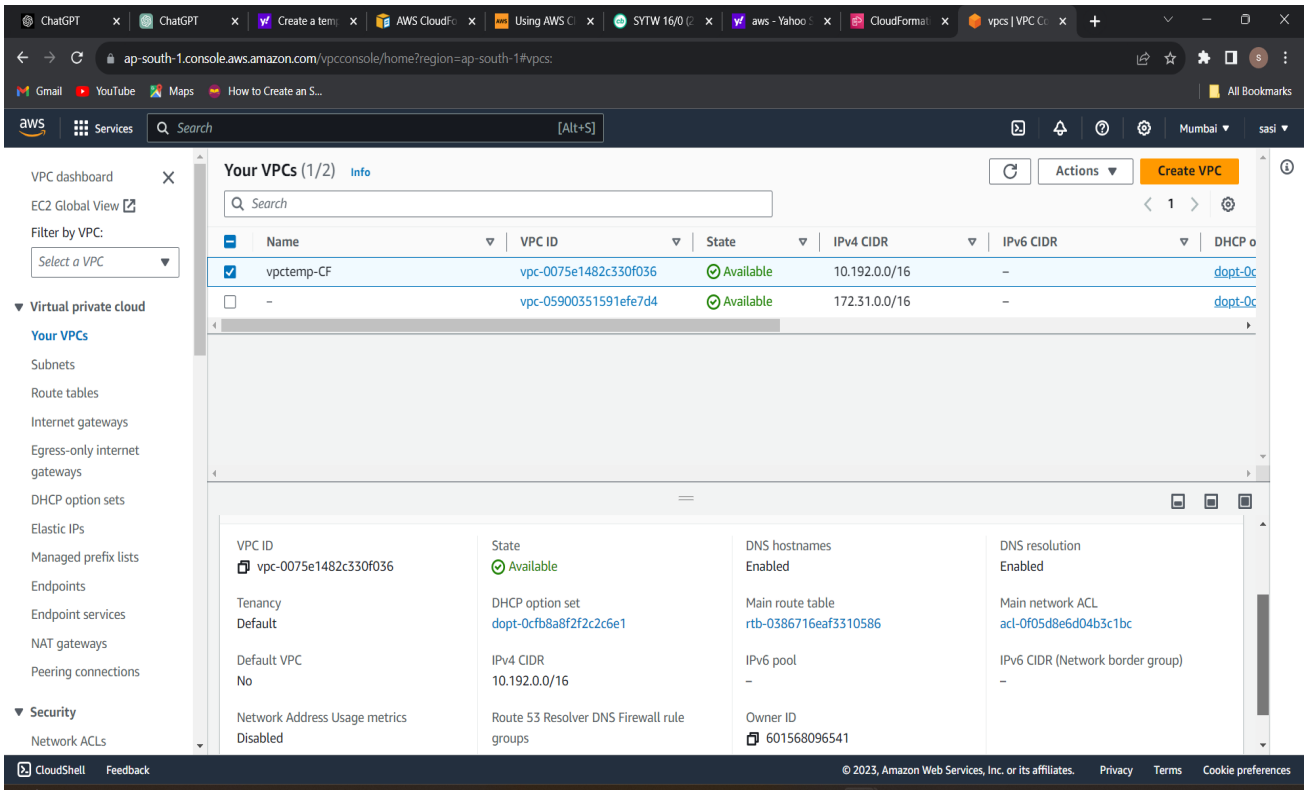

ap-south-1.console.aws.amazon.com/cloudformation/home?region=ap-south-1#/stacks/create
vpc
Step 2
Specify stack details
Step 3
Configure stack options
Step 4
Review
Prerequisite - Prepare template
Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.
Template is ready
Use a sample template
Create template in Designer
Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.
Template source
Selecting a template generates an Amazon S3 URL where it will be stored.
Amazon S3 URL
Upload a template file
Upload a template file
Choose file
CF VPC SUBNET.yml
JSON or YAML formatted file
S3 URL: https://s3.ap-south-1.amazonaws.com/cf-templates-held5lwfk2cw-ap-south-1/2023-11-15T040021.602Zs03-CFVPCSUBNET.yml
View in Designer
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

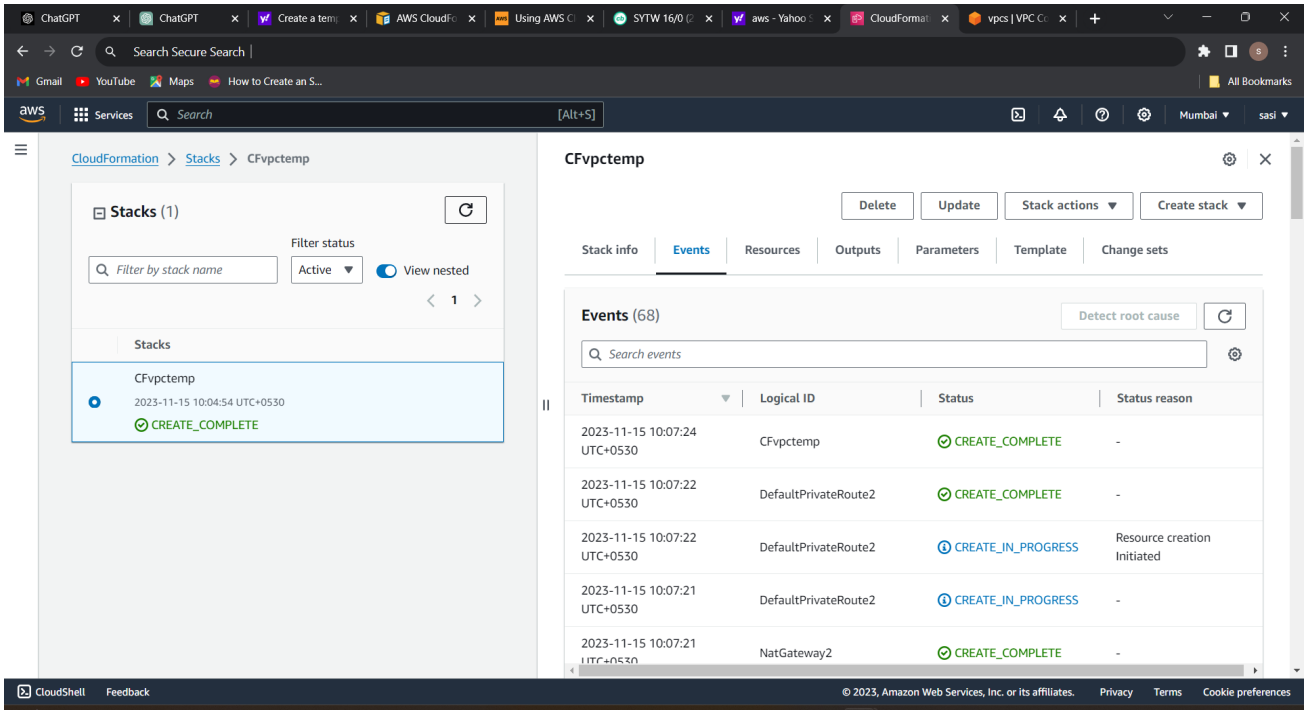

ap-south-1.console.aws.amazon.com/cloudformation/home?region=ap-south-1#/stacks/create
vpc
Use deletion policy
Retains or deletes created resources according to their attached deletion policy.
Delete all newly created resources
Deletes created resources during a rollback regardless of their attached deletion policy.
Advanced options
You can set additional options for your stack, like notification options and a stack policy. Learn more
Stack policy
Defines the resources that you want to protect from unintentional updates during a stack update.
Rollback configuration
Specify alarms for CloudFormation to monitor when creating and updating the stack. If the operation breaches an alarm threshold, CloudFormation rolls it back.
Notification options
Stack creation options
Cancel
Previous
Next
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

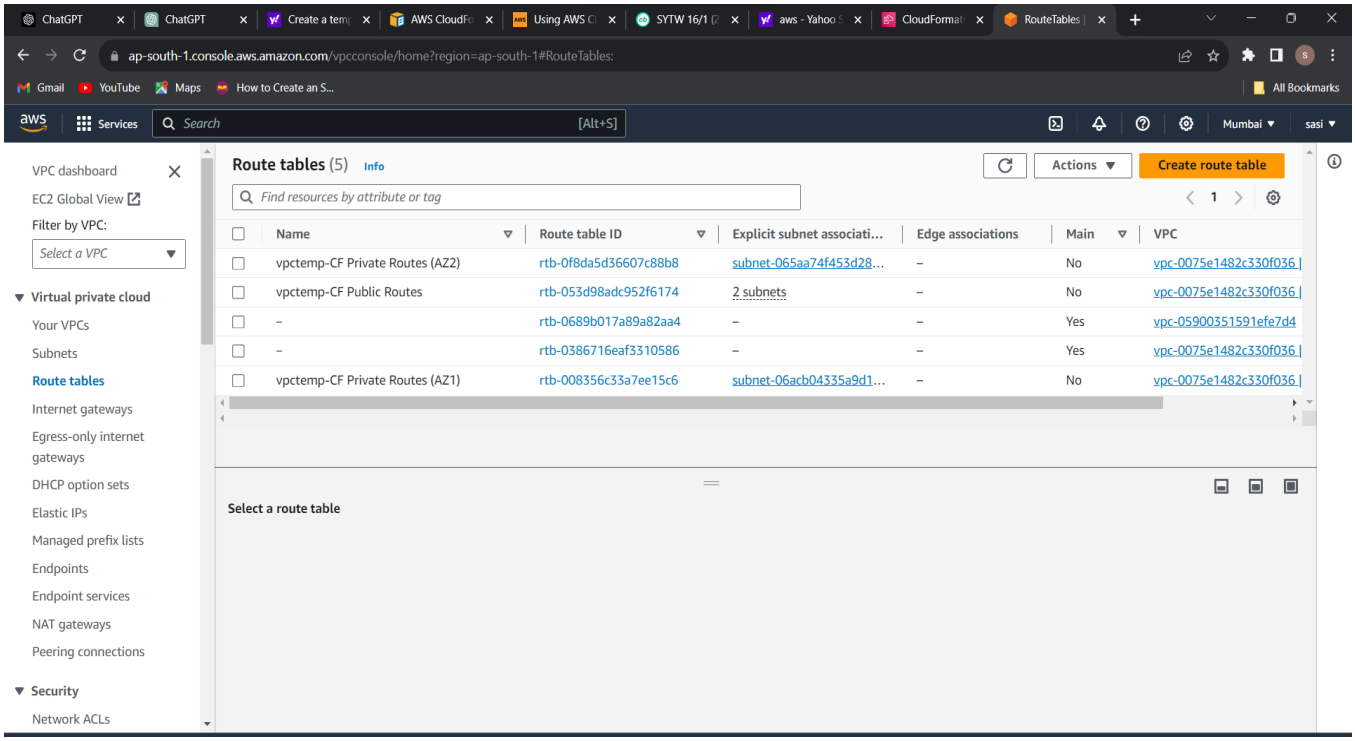

ap-south-1.console.aws.amazon.com/cloudformation/home?region=ap-south-1#/stacks/events?stackId=arn%3Aaws%3Acloudformation%3Aap-south-1%3A457228467332%3Astack%2FVPCt...
Gmail
YouTube
Maps
How to Create an S...
All Bookmarks
aws
Services
vpc
Mumbai
Sasi
CloudFormation > Stacks > VPCtemplate
Stacks (1)
Filter by stack name
Active
View nested
1
Stacks
VPCtemplate
2023-11-15 09:31:34 UTC+0530
CREATE_IN_PROGRESS
VPCtemplate
Delete
Update
Stack actions
Create stack
Stack info
Events
Resources
Outputs
Parameters
Template
Change sets
Events (3)
Detect root cause
Search events
Timestamp
Logical ID
Status
Status reason
2023-11-15 09:31:37 UTC+0530
MyVPC
CREATE_IN_PROGRESS
Resource creation Initiated
2023-11-15 09:31:36 UTC+0530
MyVPC
CREATE_IN_PROGRESS
-
2023-11-15 09:31:34 UTC+0530
VPCtemplate
CREATE_IN_PROGRESS
User Initiated
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

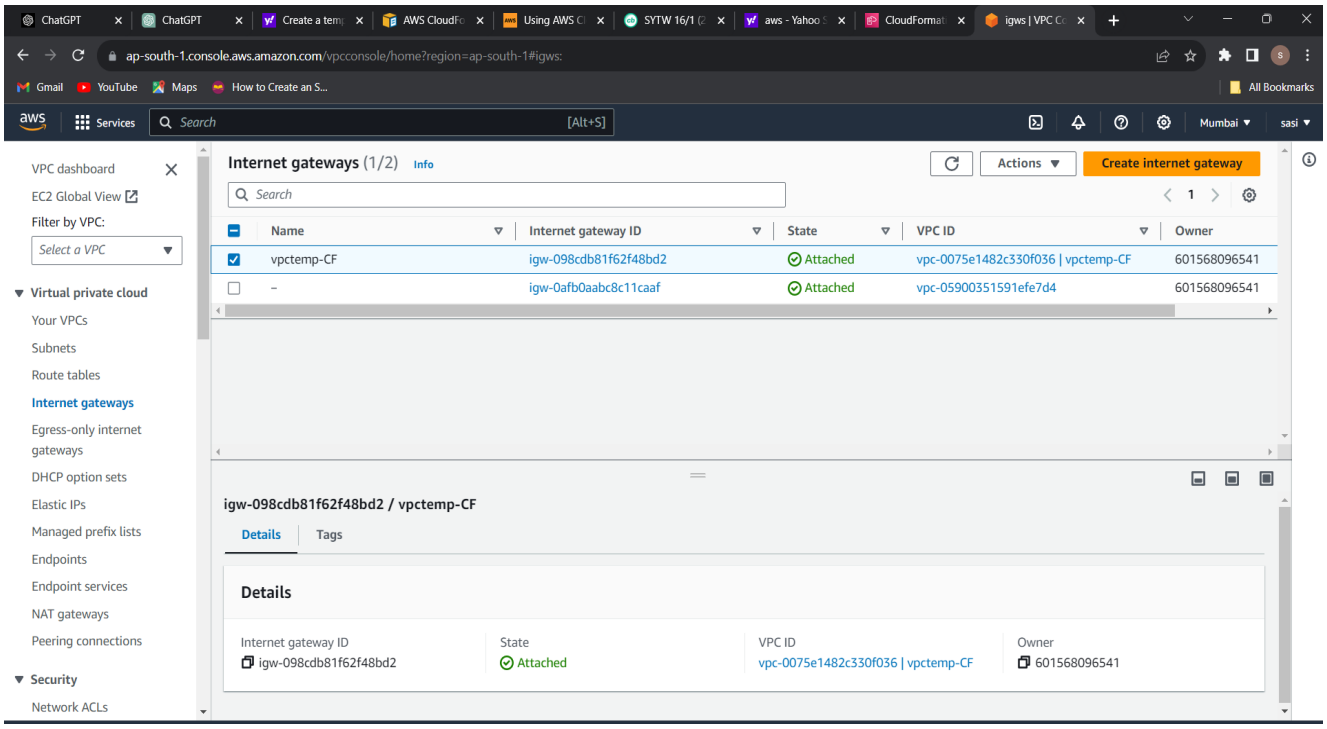

ap-south-1.console.aws.amazon.com/cloudformation/home?region=ap-south-1#/stacks/create
Gmail
YouTube
Maps
How to Create an S...
All Bookmarks
aws
Services
vpc
Mumbai
Sasi
EnvironmentName
An environment name that is prefixed to resource names
Vpctemp
PrivateSubnet1CIDR
Please enter the IP range (CIDR notation) for the private subnet in the first Availability Zone
10.192.20.0/24
PrivateSubnet2CIDR
Please enter the IP range (CIDR notation) for the private subnet in the second Availability Zone
10.192.21.0/24
PublicSubnet1CIDR
Please enter the IP range (CIDR notation) for the public subnet in the first Availability Zone
10.192.10.0/24
PublicSubnet2CIDR
Please enter the IP range (CIDR notation) for the public subnet in the second Availability Zone
10.192.11.0/24
VpcCIDR
Please enter the IP range (CIDR notation) for this VPC
10.192.0.0/16
Cancel
Previous
Next
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

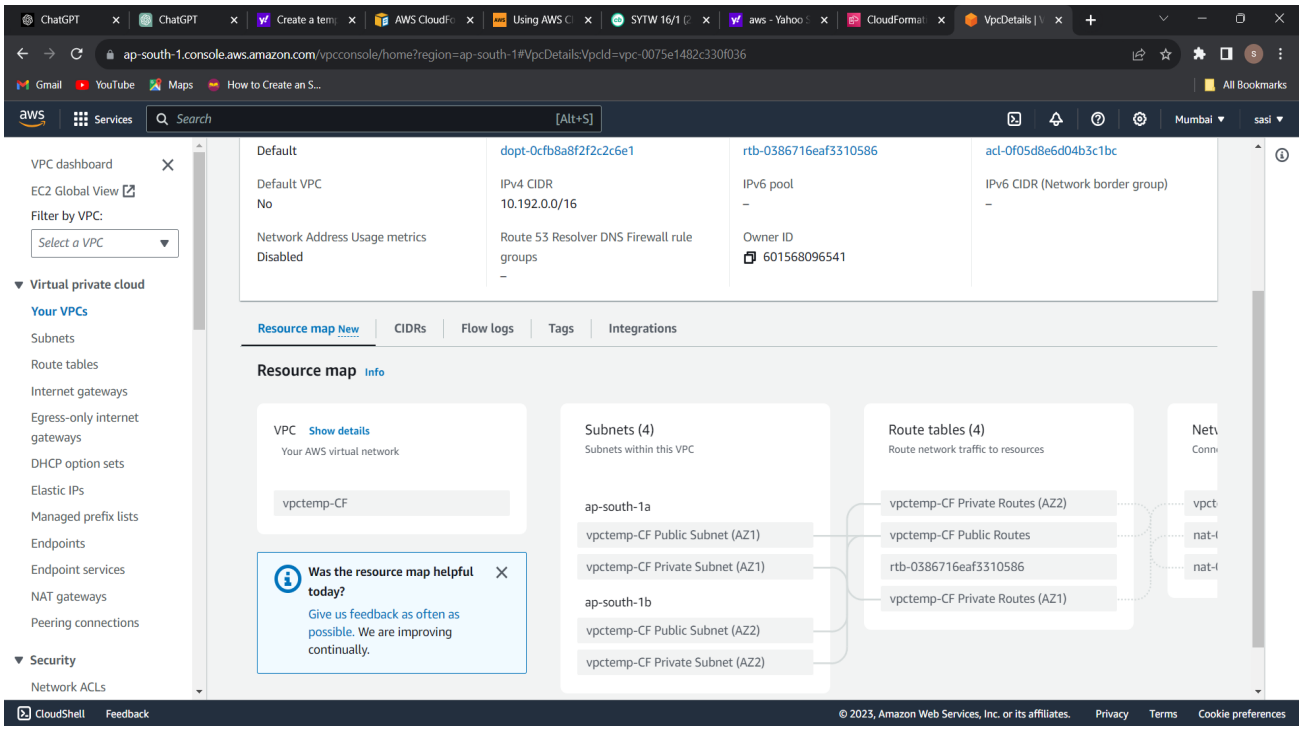

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#subnets:
Subnets (7) Info
Actions
Create subnet
Find resources by attribute or tag
Name
Subnet ID
State
VPC
IPv4 CIDR
subnet-0218af047ce3c1038 Available vpc-05900351591efe7d4 172.31.32.0/20
vpctemp-CF Private Subnet (AZ2) subnet-065aa74f453d28273 Available vpc-0075e1482c330f036 | vpct... 10.192.21.0/24
vpctemp-CF Private Subnet (AZ1) subnet-06acb04335a9d1a94 Available vpc-0075e1482c330f036 | vpct... 10.192.20.0/24
vpctemp-CF Public Subnet (AZ2) subnet-09d4dda116f7de542 Available vpc-0075e1482c330f036 | vpct... 10.192.11.0/24
subnet-05e13e0f014be0f7b Available vpc-05900351591efe7d4 172.31.0.0/20
vpctemp-CF Public Subnet (AZ1) subnet-0b7e1bd15d44ce134 Available vpc-0075e1482c330f036 | vpct... 10.192.10.0/24
Select a subnet
VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

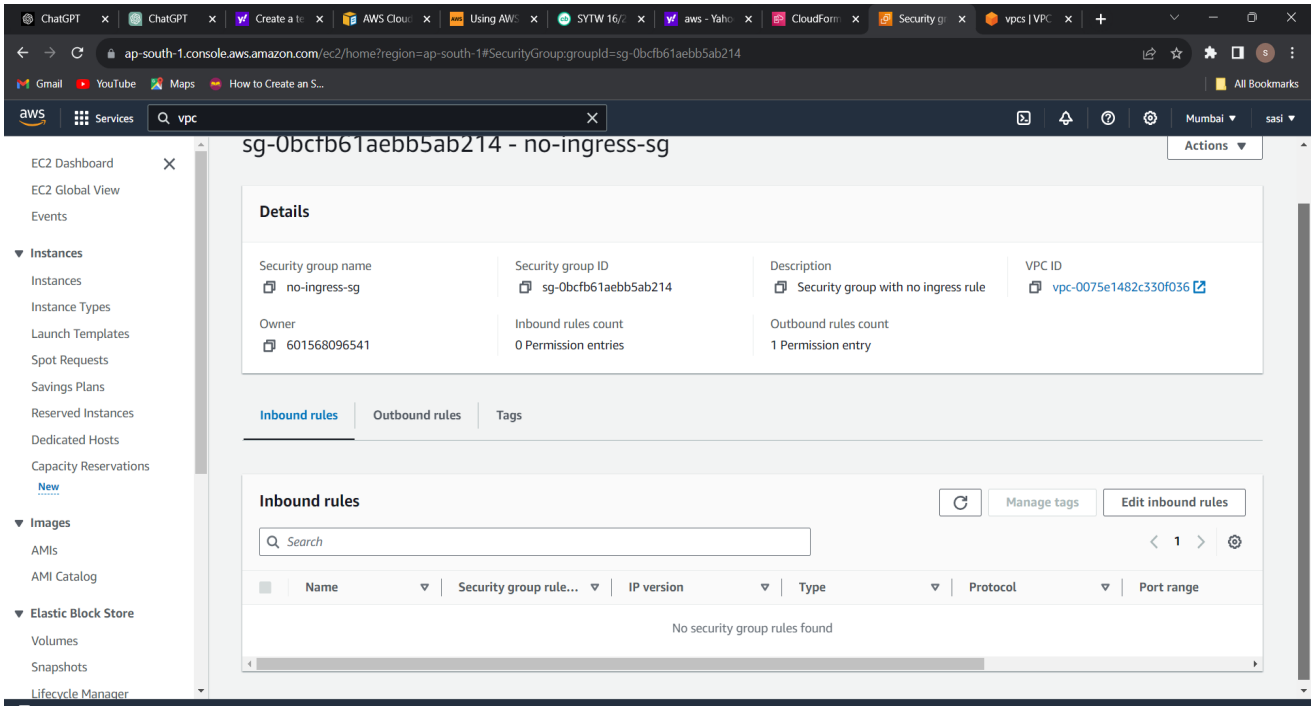

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#vpcs:
Your VPCs (1/2) Info
Actions
Create VPC
Search
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
vpctemp-CF vpc-0075e1482c330f036 Available 10.192.0.0/16 –
– vpc-05900351591efe7d4 Available 172.31.0.0/16 –
VPC ID
vpc-0075e1482c330f036
State
Available
DNS hostnames
Enabled
DNS resolution
Enabled
Tenancy
Default
DHCP option set
dopt-0cfb8a8f2f2c2c6e1
Main route table
rtb-0386716eaf3310586
Main network ACL
acl-0f05d8e6d04b3c1bc
Default VPC
No
IPv4 CIDR
10.192.0.0/16
IPv6 pool
–
IPv6 CIDR (Network border group)
–
Network Address Usage metrics
Disabled
Route 53 Resolver DNS Firewall rule groups
Owner ID
601568096541
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


CloudFormation > Stacks > CFvpctemp
Stacks (1)
Filter by stack name
Active
View nested
Stacks
CFvpctemp
2023-11-15 10:04:54 UTC+0530
CREATE_COMPLETE
CFvpctemp
Delete
Update
Stack actions
Create stack
Stack info
Events
Resources
Outputs
Parameters
Template
Change sets
Events (68)
Detect root cause
Search events
Timestamp
Logical ID
Status
Status reason
2023-11-15 10:07:24 UTC+0530
CFvpctemp
CREATE_COMPLETE
2023-11-15 10:07:22 UTC+0530
DefaultPrivateRoute2
CREATE_COMPLETE
2023-11-15 10:07:22 UTC+0530
DefaultPrivateRoute2
CREATE_IN_PROGRESS
Resource creation Initiated
2023-11-15 10:07:21 UTC+0530
DefaultPrivateRoute2
CREATE_IN_PROGRESS
2023-11-15 10:07:21
NatGateway2
CREATE_COMPLETE
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

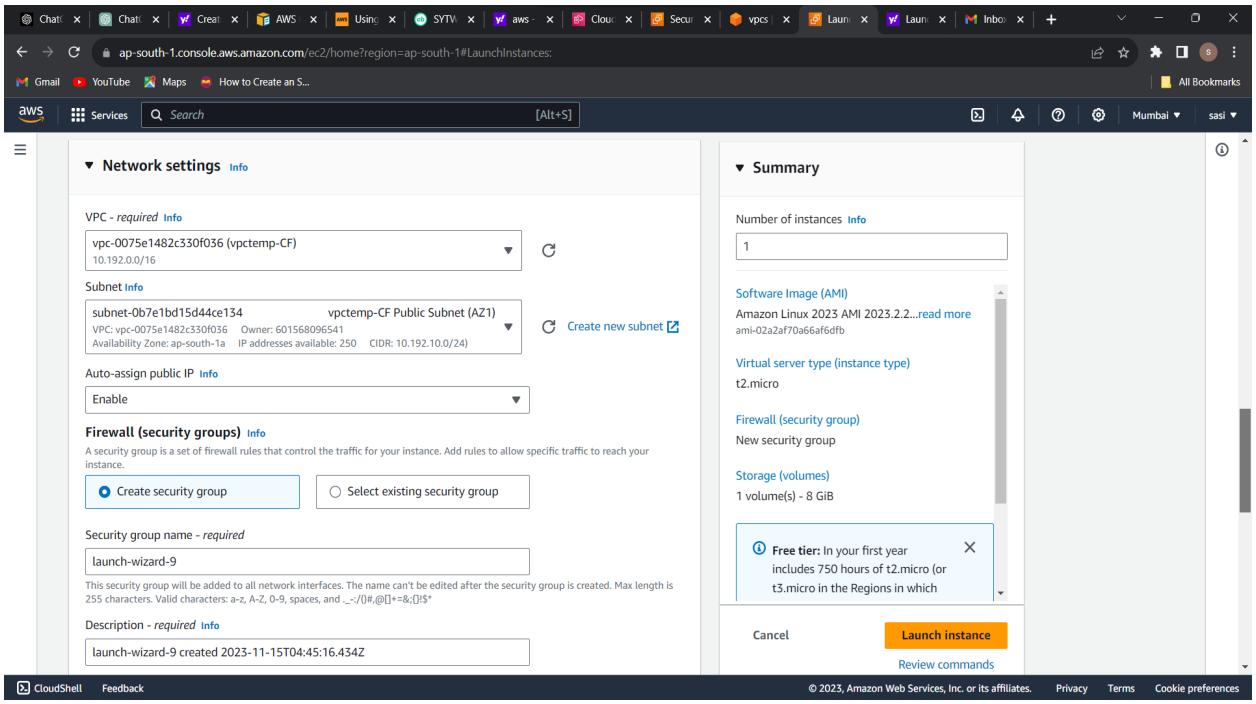

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTables:
VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Route tables (5) Info
Find resources by attribute or tag
Actions
Create route table
Name
Route table ID
Explicit subnet associati...
Edge associations
Main
VPC
vpctemp-CF Private Routes (AZ2)
rtb-0f8da5d36607c88b8
subnet-065aa74f453d28...
No
vpctemp-CF Public Routes
rtb-053d98adc952f6174
2 subnets
No
rtb-0689b017a89a82aa4
Yes
vpc-05900351591efe7d4
rtb-0386716eaf3310586
Yes
vpctemp-CF Private Routes (AZ1)
rtb-008356c33a7ee15c6
subnet-06acb04335a9d1...
No
Select a route table

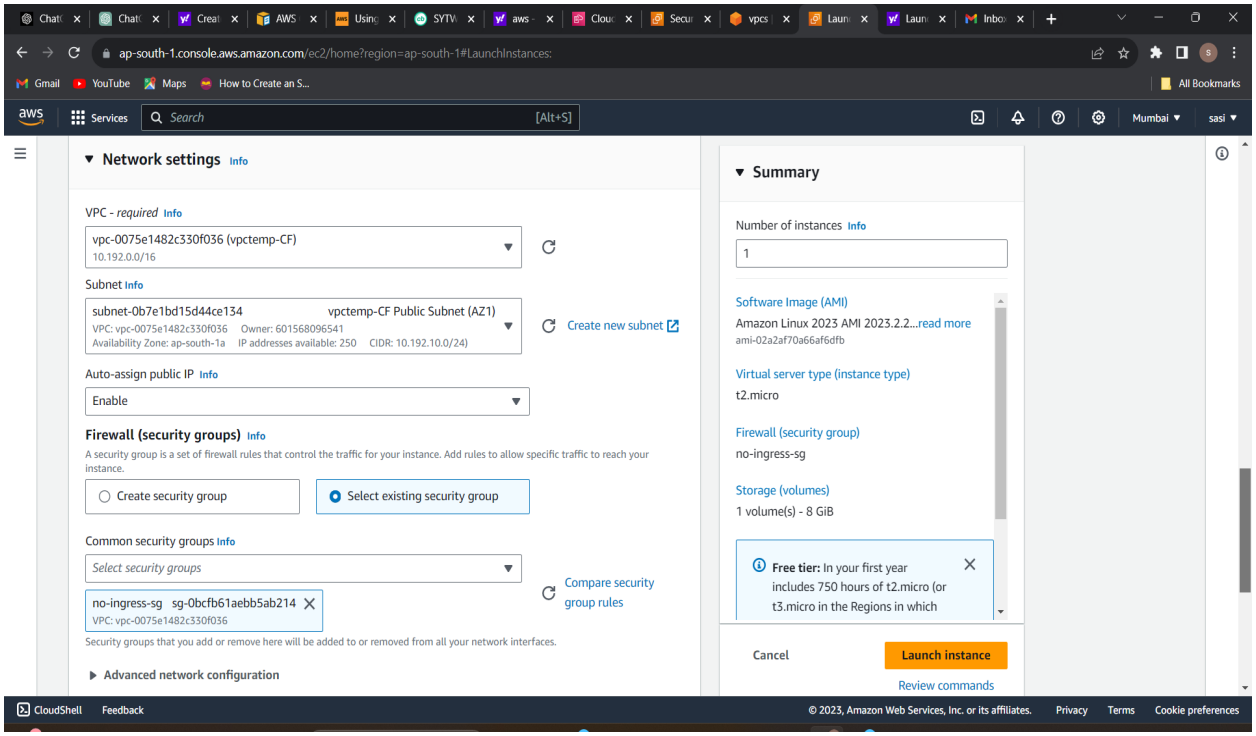

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#igws:
Internet gateways (1/2) Info
Actions
Create internet gateway
Search
Name
Internet gateway ID
State
VPC ID
Owner
vpctemp-CF
igw-098cdb81f62f48bd2
Attached
vpc-0075e1482c330f036 | vpctemp-CF
601568096541
igw-0afb0aabc8c11caaf
Attached
vpc-05900351591efe7d4
601568096541
VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
igw-098cdb81f62f48bd2 / vpctemp-CF
Details
Tags
Details
Internet gateway ID
igw-098cdb81f62f48bd2
State
Attached
VPC ID
vpc-0075e1482c330f036 | vpctemp-CF
Owner
601568096541

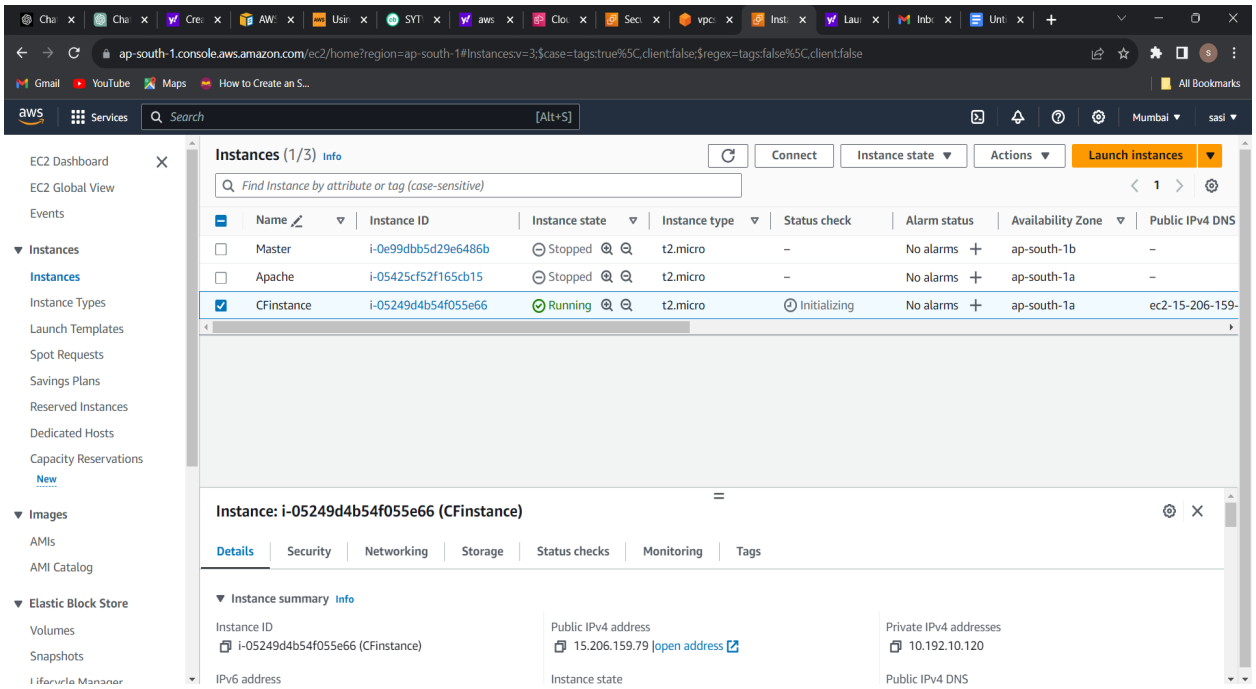

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#VpcDetails:VpcId=vpc-0075e1482c330f036
Default
dopt-0cfb8a8f2f2c2c6e1
rtb-0386716eaf3310586
acl-0f05d8e6d04b3c1bc
Default VPC
No
IPv4 CIDR
10.192.0.0/16
IPv6 pool
–
IPv6 CIDR (Network border group)
–
Network Address Usage metrics
Disabled
Route 53 Resolver DNS Firewall rule groups
–
Owner ID
601568096541
Resource map New
CIDRs
Flow logs
Tags
Integrations
Resource map Info
VPC Show details
Your AWS virtual network
vpctemp-CF
Subnets (4)
Subnets within this VPC
ap-south-1a
vpctemp-CF Public Subnet (AZ1)
vpctemp-CF Private Subnet (AZ1)
ap-south-1b
vpctemp-CF Public Subnet (AZ2)
vpctemp-CF Private Subnet (AZ2)
Route tables (4)
Route network traffic to resources
vpctemp-CF Private Routes (AZ2)
vpctemp-CF Public Routes
rtb-0386716eaf3310586
vpctemp-CF Private Routes (AZ1)
Was the resource map helpful today?
Give us feedback as often as possible. We are improving continually.
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



Using above VPC and public subnet and security group i had created one EC2 instance name CFinstance




ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
Gmail
YouTube
Maps
How to Create an S...
All Bookmarks
aws
Services
Search
[Alt+S]
Mumbai
sasi
Network settings Info
VPC - required Info
vpc-0075e1482c330f036 (vpctemp-CF)
10.192.0.0/16
Subnet Info
subnet-0b7e1bd15d44ce134 vpctemp-CF Public Subnet (AZ1)
VPC: vpc-0075e1482c330f036 Owner: 601568096541
Availability Zone: ap-south-1a IP addresses available: 250 CIDR: 10.192.10.0/24)
Create new subnet
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
no-ingress-sg sg-0bcfb61aebb5ab214
VPC: vpc-0075e1482c330f036
Compare security group rules
Security groups that you add or remove here will be added to or removed from all your network interfaces.
Advanced network configuration
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.2.2...read more
ami-02a2af70a66af6dfb
Virtual server type (instance type)
t2.micro
Firewall (security group)
no-ingress-sg
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 which
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Instances:v=3;$case=tags:true%5C,client:false;$regex=tags:false%5C,client:false
Gmail
YouTube
Maps
How to Create an S...
All Bookmarks
aws
Services
Search
[Alt+S]
Mumbai
sasi
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Instances (1/3) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Master
i-0e99dbb5d29e6486b
Stopped
t2.micro
–
No alarms
ap-south-1b
–
Apache
i-05425cf52f165cb15
Stopped
t2.micro
–
No alarms
ap-south-1a
–
CFinstance
i-05249d4b54f055e66
Running
t2.micro
Initializing
No alarms
ap-south-1a
ec2-15-206-159-
Instance: i-05249d4b54f055e66 (CFinstance)
Details
Security
Networking
Storage
Status checks
Monitoring
Tags
Instance summary Info
Instance ID
i-05249d4b54f055e66 (CFinstance)
Public IPv4 address
15.206.159.79 |open address
Private IPv4 addresses
10.192.10.120
IPv6 address
Instance state
Public IPv4 DNS