PROJECT2:

AWS Routing & Switching using CentOS Server Administration

16.10.2024

Prepared By:

K. Dushyant Reddy

Guided By:

Zakir Hussain

INDEX

OBJECTIVE

The primary objective of implementing and maintaining a switch and routing network in AWS using CentOS server administration for a centralized large network is to establish a robust, secure, and highly available network infrastructure that can efficiently manage and monitor all traffic flowing through the environment. This centralized network architecture aims to provide a single pane of glass for administrators to control and inspect all ingress and egress traffic, thereby enhancing network security and reducing the risk of unauthorized access.

Additionally, this architecture enables better monitoring and troubleshooting capabilities, allowing administrators to quickly identify and resolve issues, thereby minimizing downtime and ensuring high network availability. Overall, the objective is to create a scalable, flexible, and secure network infrastructure that can support the growing demands of a large network, while also providing a solid foundation for future network expansion and development.

INTRODUCTION

Implementing and maintaining a switch and routing network in AWS using CentOS server administration is crucial for a large-scale network. Amazon Web Services (AWS) provides a robust platform for building and managing a switch and routing network, and CentOS server administration can be used to centrally manage and monitor the network infrastructure. The benefits of implementing a switch and routing network in AWS include scalability, security, high availability, and centralized management. A virtual private cloud (VPC) is a virtual network dedicated to the AWS account, providing a secure and isolated environment for the network infrastructure. Subnets, route tables, switches, routers, and EC2 instances running CentOS are key components of a switch and routing network in AWS.

CentOS server administration plays a vital role in centralized network management. It can be used to configure and manage network interfaces, routing tables, and firewall rules. Additionally, CentOS can be used to monitor and log network activity, providing real-time insights into network performance and security. Automation and scripting can also be used to automate network tasks and scripts, making it easier to manage and maintain the network infrastructure. By implementing a switch and routing network in AWS using CentOS server administration, organizations can build

a scalable, secure, and highly available network infrastructure that can be centrally managed and monitored. This approach enables organizations to efficiently manage their network resources, reduce costs, and improve overall network performance.

In a large-scale network, a switch and routing network is essential for efficient communication, scalability, and security. AWS provides a highly scalable infrastructure that can easily adapt to growing network demands. The use of CentOS server administration provides a centralized management system, making it easier to troubleshoot and resolve issues. The combination of AWS and CentOS server administration provides a robust and secure network infrastructure that can meet the demands of a large-scale network. By leveraging the benefits of AWS and CentOS server administration, organizations can build a network infrastructure that is highly available, scalable, and secure.

PREREQUISITES

Basic knowledge on -

1. **Amazon VPC (Virtual Private Cloud)** - Isolated virtual network environment within AWS, allowing customization of network settings and security configurations.

   Subnet - Segments of a VPC, dividing the network into smaller, manageable parts. Subnets can be public (accessible from the internet) or private (isolated from the internet).

2. **IAM(Identity and Access Management)** - solution that enables to manage users' access to AWS resources.

3. **Amazon EC2 (Elastic Compute Cloud)** - Web service which provides resizable compute capacity in the cloud.

   Instance - Virtual computing environments

4. **AWS RDS (Relational Database Service)** - Managed relational database service, providing easy setup, scaling, and maintenance of SQL databases like MySQL, PostgreSQL, etc.

5. **Elastic Load Balancing** - manages the workload on the instances and distributes them to other instances in case of an instance failure.

   Application Load Balancers - Ideal for routing HTTP/HTTPS traffic and performing advanced traffic routing and content-based routing.

6. **Auto Scaling** - helps you maintain application availability and allows you to automatically add or remove Amazon EC2 instances according to conditions you define.

7. **AMI (Amazon Machine Image)** - an image that provides the software that is required to set up and boot an Amazon EC2 instance.

8. **AWS Transit Gateway** - a network transit hub that you can use to interconnect your virtual private clouds (VPCs) and on-premises networks

9. **AWS Systems Manager** - helps to manage applications and infrastructure running in the AWS. It simplifies application and resource management, shortens the time to detect, resolve operational problems, and helps to manage AWS resources securely at scale

10. **Amazon S3 (Simple Storage Service)** - a highly scalable object storage service used for a wide range of storage solutions, including websites, mobile applications, backups, and data lakes.

11. **Amazon SNS (Simple Notification Service)** - a managed service that provides message delivery from publishers to subscribers

12. **Amazon CloudWatch** - used to collect and track metrics, which are variables that can be measured for the resources and application.

13. **AWS Cost Explorer** - a tool that enables you to view and analyze your costs and usage

14. **Budgets** - lets you set custom cost and usage budgets that alert you when your budget thresholds are exceeded (or forecasted to exceed)

15. **AWS Cost and Usage Report** - tracks your AWS usage and provides estimated charges associated with your account.

REAL-TIME SCENARIO

Scenario: Centralized Network for a Large E-Commerce Company

Company Background:

Founded in 2010, TechRev is a rapidly growing e-commerce company that started as a small online retail store specializing in electronics. Over the years, it expanded its offerings to include clothing, home appliances, and beauty products. As the customer base grew globally, TechRev invested heavily in its digital transformation to accommodate millions of daily users and support its expanding catalog. The company's infrastructure now spans multiple departments, including marketing, sales, customer support, development, and logistics. Each department relies on various applications and services to manage day-to-day operations, customer interactions, and business growth.

Current Scenario:

To establish a centralized network infrastructure in AWS to unify the company's fragmented systems and services into a cohesive and manageable network. The infrastructure will efficiently manage traffic across departments, ensure secure communication between services, and provide VPN access for remote employees, enabling seamless collaboration. This centralized approach aims to enhance network security, improve monitoring capabilities, and support future growth. Problems faced:

- Siloed Infrastructure: Each department had its own set of services hosted on different cloud providers and on-premises servers, leading to inefficiencies, integration issues, and high maintenance costs.
- Security Concerns: With no unified security framework, the company faced risks of data breaches, as different teams managed separate security protocols and policies.

- High Operational Costs: Running multiple fragmented systems resulted in excessive costs for hardware, software licenses, and maintenance.
- Scalability Issues: Handling increased traffic during sales events like "Black Friday" was challenging due to the limited scalability of the existing on-premises servers.
- Complex Troubleshooting: With systems scattered across different environments, identifying and resolving network issues often took longer, causing potential revenue loss due to downtime.

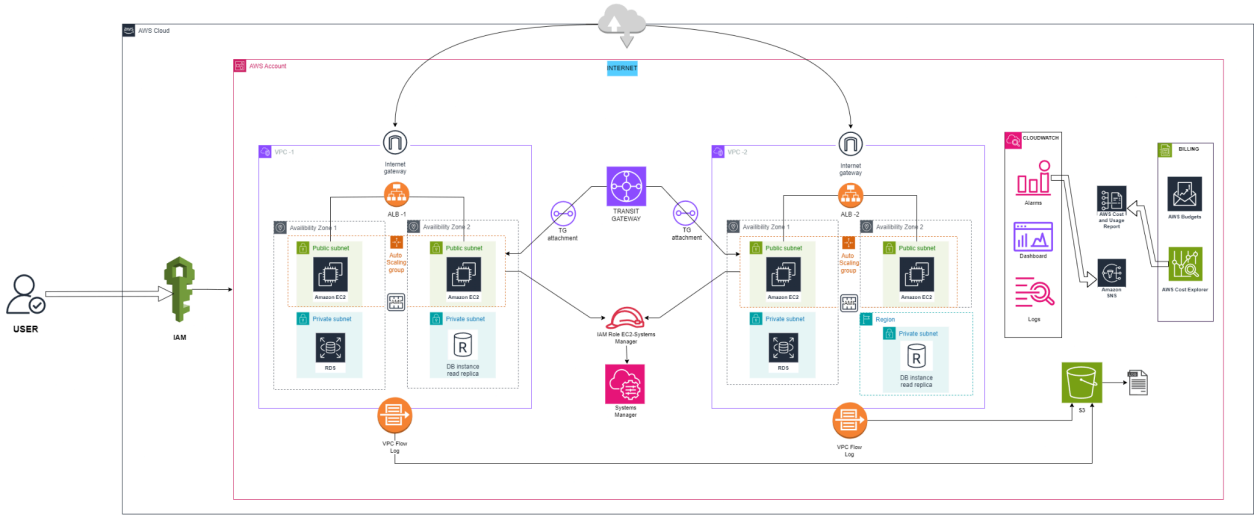
Solution:

The solution involves implementing a centralized network using AWS services to consolidate all departmental infrastructures, allowing TechRev to efficiently manage traffic, enhance security, and support scalability.

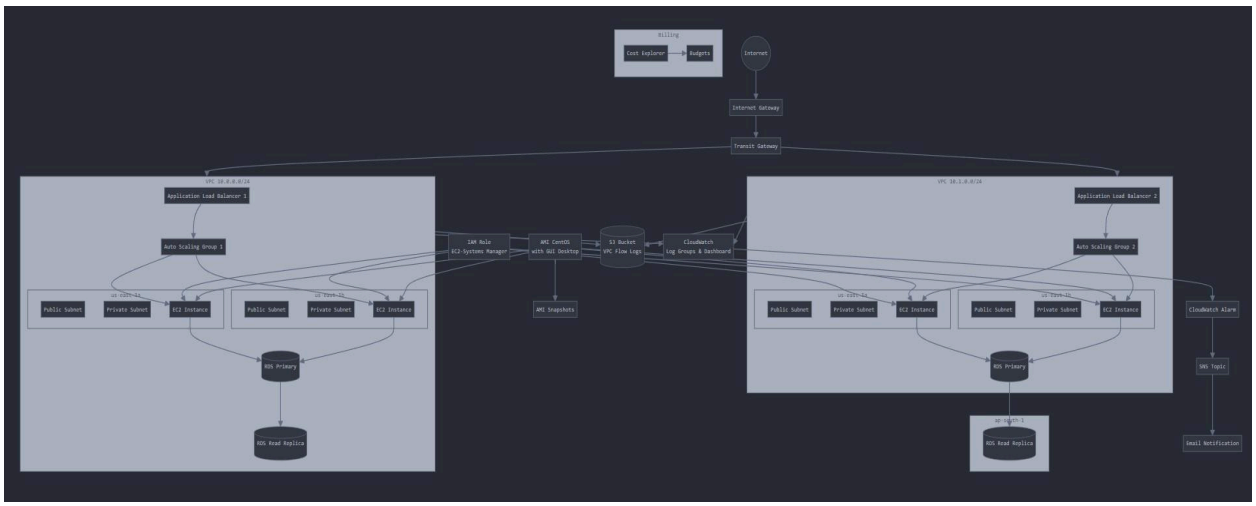
Benefits:

- Increased Security: By unifying security policies and consolidating resources within AWS, the risk of breaches is significantly reduced.
- Operational Cost Savings: With a pay-as-you-go model, TechRev can eliminate the expenses associated with maintaining separate infrastructures.
- Scalability for Growth: The new architecture supports seamless scaling during peak times, ensuring that users experience consistent performance.
- Improved Troubleshooting: Centralized logging and monitoring allow for quicker identification and resolution of issues.
- Efficient Collaboration: A unified infrastructure ensures that all departments can easily share data.

ARCHITECTURE DIAGRAM



AWS Routing & Switching Server Configuration Arch Diagram



AWS Routing & Switching Server Configuration Flow Diagram

Data Flow:

This architecture represents an AWS architecture with an Application Load Balancer serving as the entry point to the system. Behind the Load Balancer, an Auto Scaling Group provides high availability by scaling the number of EC2 instances up or down based on demand.

The EC2 instances, running the AMI CentOS with GUI Desktop, are launched in a private subnet for security purposes and communicate with a database hosted by an RDS instance. The RDS instance is configured as a primary database with a read replica for redundancy and high availability.

Here's a breakdown of the architecture's key components and their roles:

- Internet Gateway: Serves as the entry point for traffic from the internet.
- Transit Gateway: This is a highly scalable and efficient way to connect multiple VPCs. It's used to connect two VPCs in this diagram.
- Application Load Balancer (ALB): The main entry point for incoming traffic. It distributes incoming traffic to healthy EC2 instances behind it.
- Auto Scaling Group: Dynamically manages the number of EC2 instances running to ensure performance and availability.
- EC2 Instances: The application servers that handle requests from the ALB. They are launched in a private subnet for enhanced security.
- Private Subnets: Subnets designed to secure internal applications and data. EC2 instances are launched in this subnet.
- Public Subnet: Subnet designed for internet-facing services. In this example, it's empty.
- RDS Primary: The primary database, responsible for writing and receiving updates.
- RDS Read Replica: A read-only replica of the primary database, offering improved read performance and availability.
- CloudWatch: AWS's monitoring service that tracks various metrics. It's used to trigger alarms and send notifications.
- CloudWatch Alarm: Configured to monitor key metrics in the system and trigger actions, like sending notifications to an SNS topic, when thresholds are breached.
- SNS Topic: A communication channel for sending notifications.
- Email Notification: Receives alerts from the SNS topic.

IMPLEMENTATION

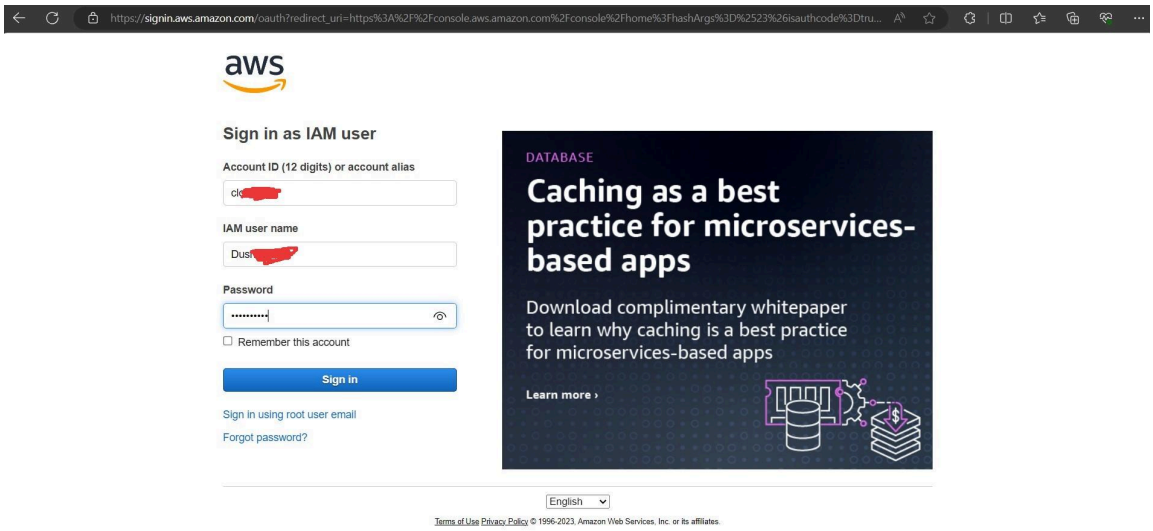
1. Console Login Configuration

Console Login Configuration:

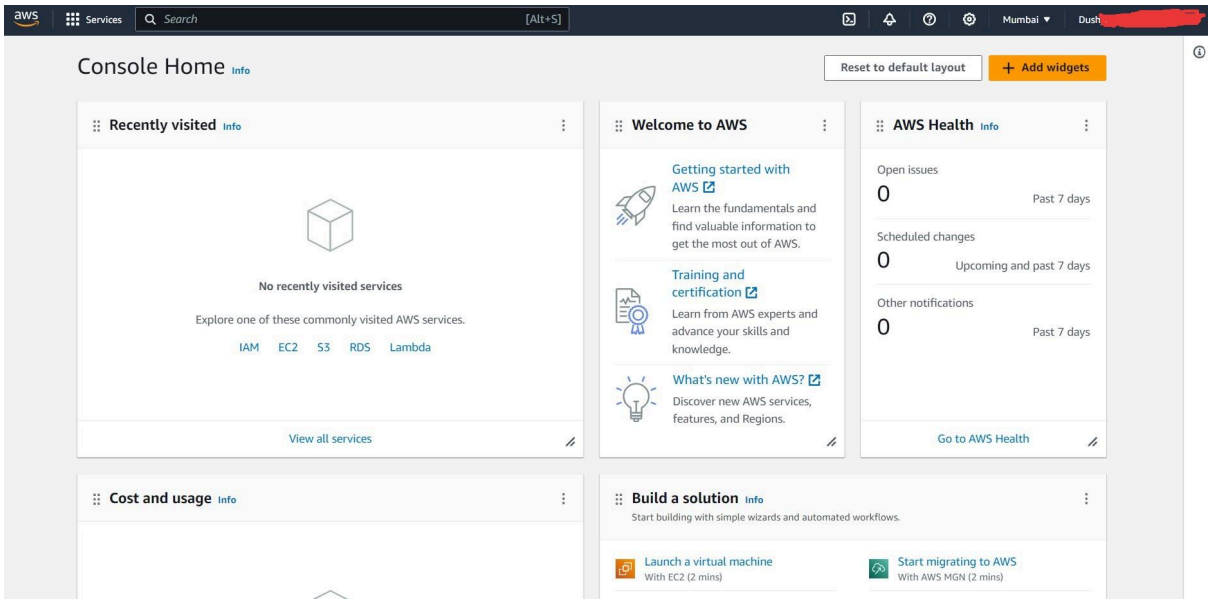
- Go to https://aws.amazon.com/console/ and click on "Sign in to the Console".
- If you're using an AWS root account, enter your email address associated with the account. If you're using an IAM user account, select "IAM user" and enter your account ID or account alias.
- Once logged in, you'll be directed to the AWS Management Console, where you can manage your AWS services.

Step 1: Login into AWS Console

1.1 Create an account and login into it by providing the credentials.



1.2 Give access to AWS Dashboard


aws
Services
Search
[Alt+S]
Mumbai
Dush
Console Home Info
Reset to default layout
+ Add widgets
Recently visited Info
No recently visited services
Explore one of these commonly visited AWS services.
IAM EC2 S3 RDS Lambda
View all services
Welcome to AWS
Getting started with AWS
Learn the fundamentals and find valuable information to get the most out of AWS.
Training and certification
Learn from AWS experts and advance your skills and knowledge.
What's new with AWS?
Discover new AWS services, features, and Regions.
AWS Health Info
Open issues
0
Past 7 days
Scheduled changes
0
Upcoming and past 7 days
Other notifications
0
Past 7 days
Go to AWS Health
Cost and usage Info
Build a solution Info
Start building with simple wizards and automated workflows.
Launch a virtual machine
With EC2 (2 mins)
Start migrating to AWS
With AWS MGN (2 mins)

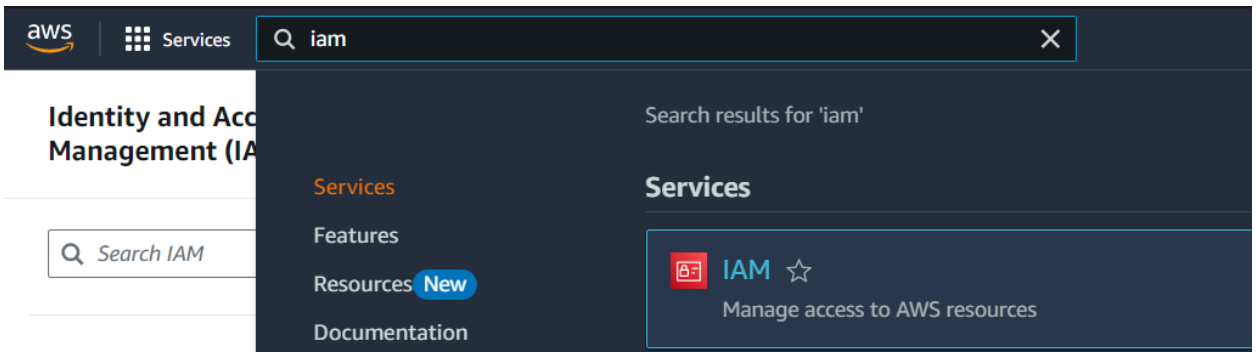
2. IAM Configuration

IAM Groups and Users Configuration:

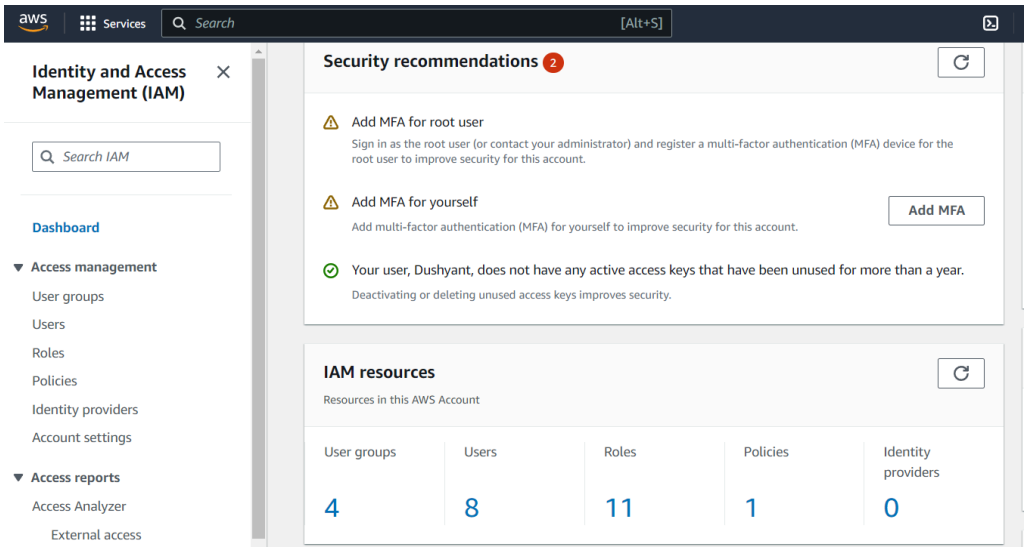
- In the IAM dashboard, select **User groups** from the left sidebar. Enter a name for the group. Attach policies to the group to define permissions
- Repeat the steps above to create 2 more groups.
- **Groups:** P2-Networking, P2-Infrastructure and P2-Monitoring
- In the IAM dashboard, select **Users** from the left sidebar. Enter a username and choose the access type AWS Console access.
- Add the user to one of the groups you created earlier.
- Repeat the steps above to create 6 more users.
- **Users:** Anuja, Anmol, Mansi, Gaurav, Mainak and Dushyant
- Then go to the Role section and create a role for EC2 and Systems Manager and give permission for AmazonSSMManagedInstanceCore and click Create Role.

Step 2: Launch IAM in Console

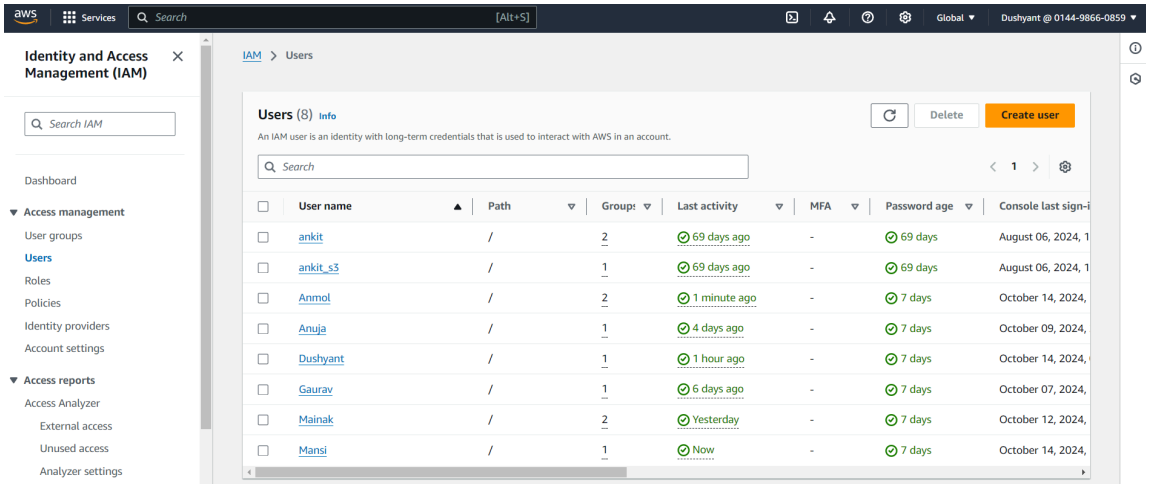
2.1 In Dashboard, search for IAM service, click **IAM** to open it.

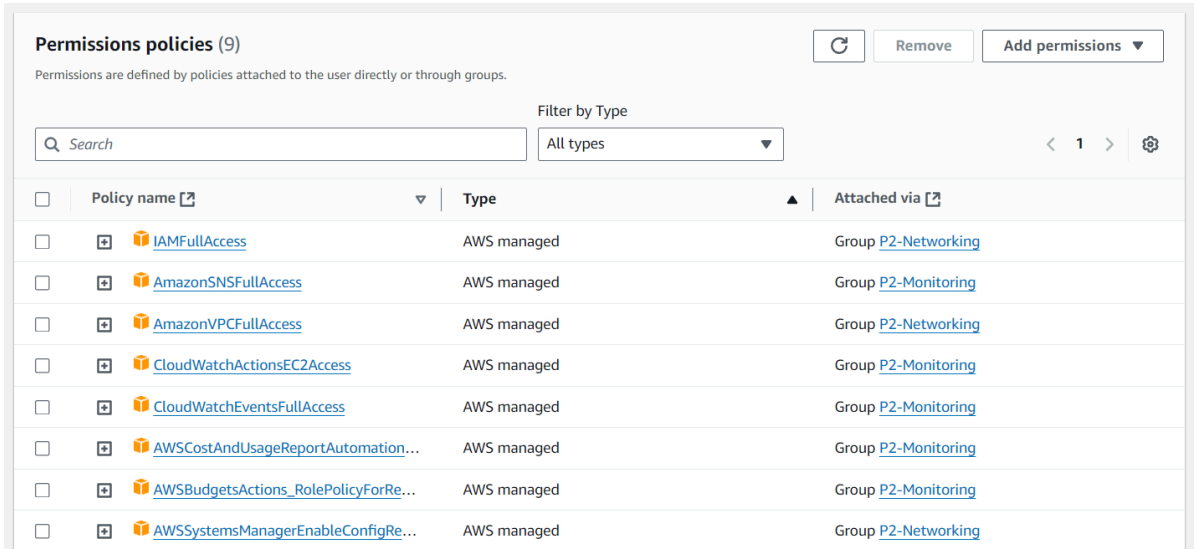


2.2 Under IAM resources, user groups and users are being assigned.

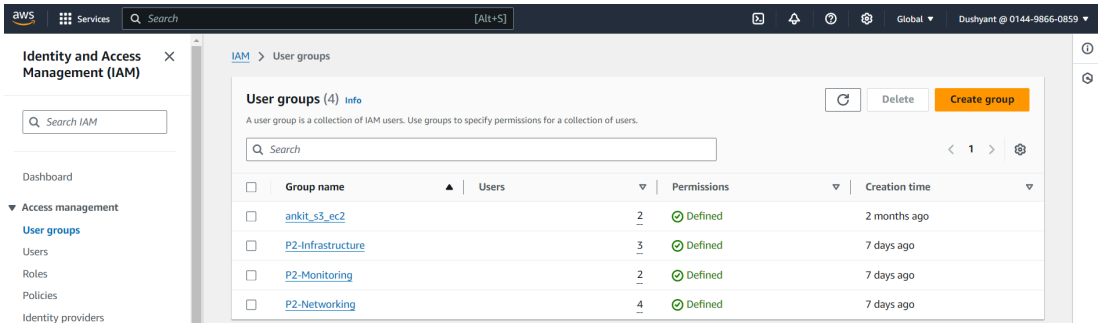


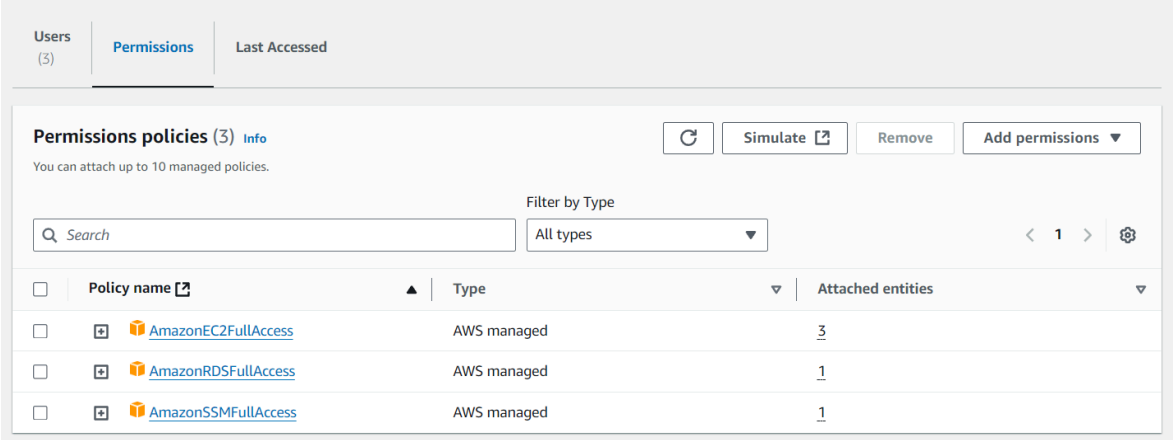
2.3 Created 6 users - Dushyant, Mainak, Mansi, Gaurav, Anuja and Anmol and added the permissions policies individually.



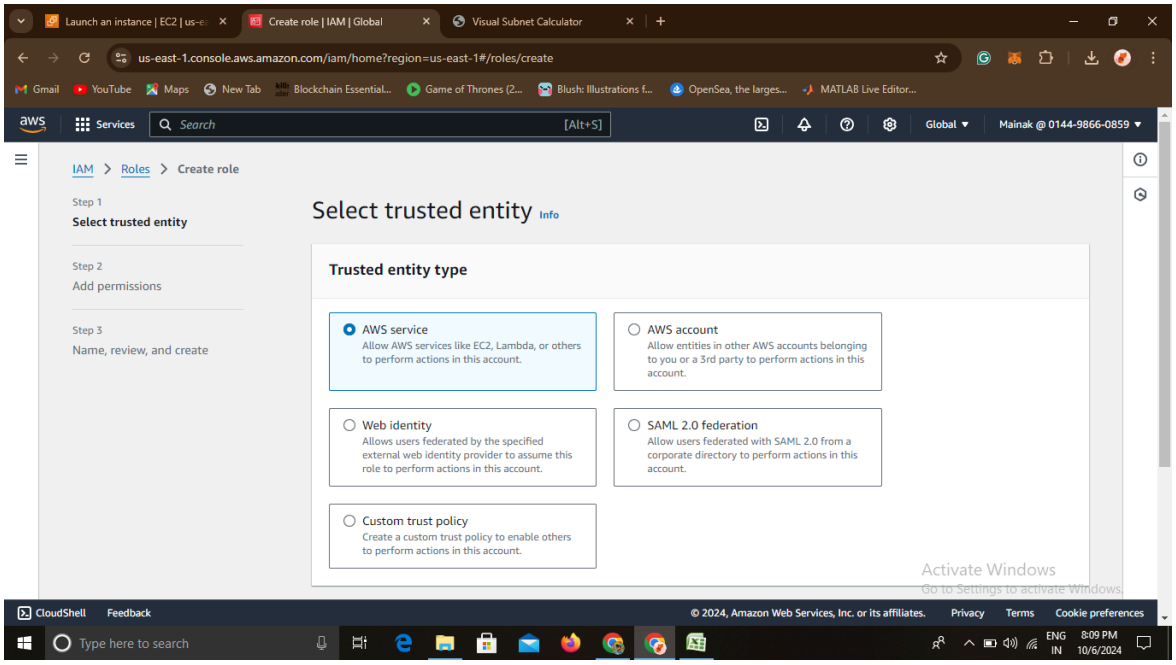


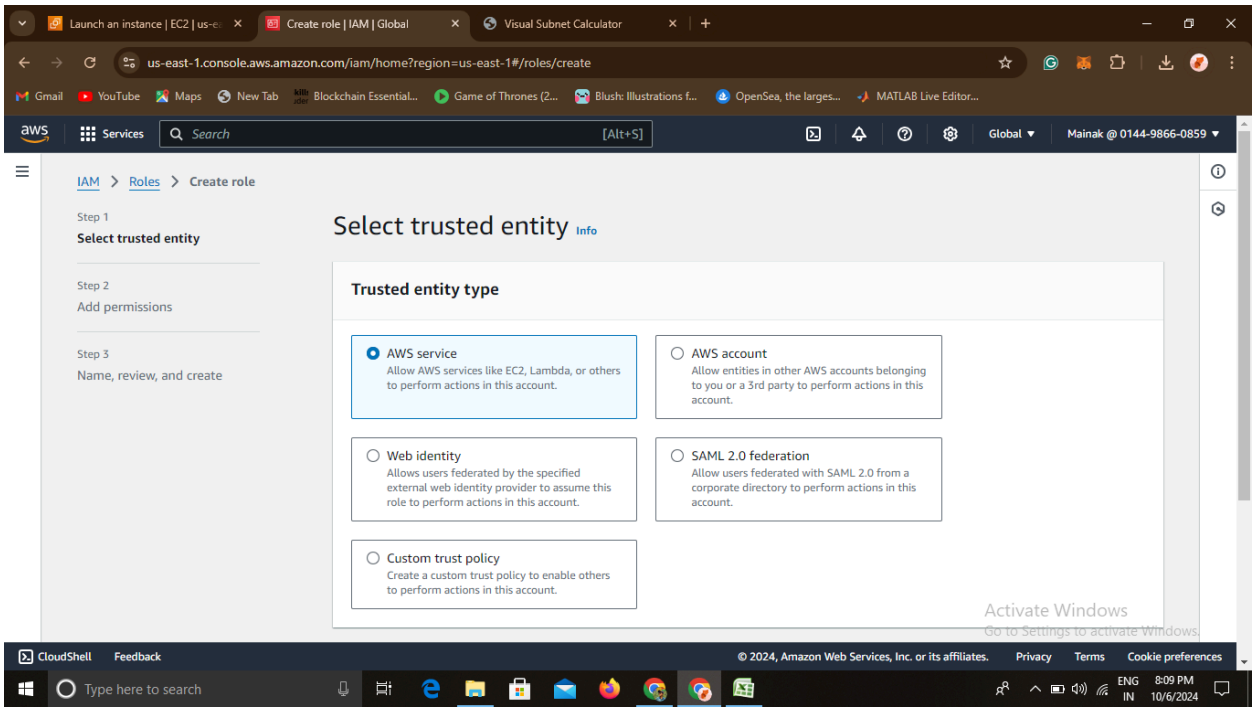
2.4 Created 3 user groups - P2-Infrastructure, P2-Monitoring and P2-Networking and attached the users with the policies



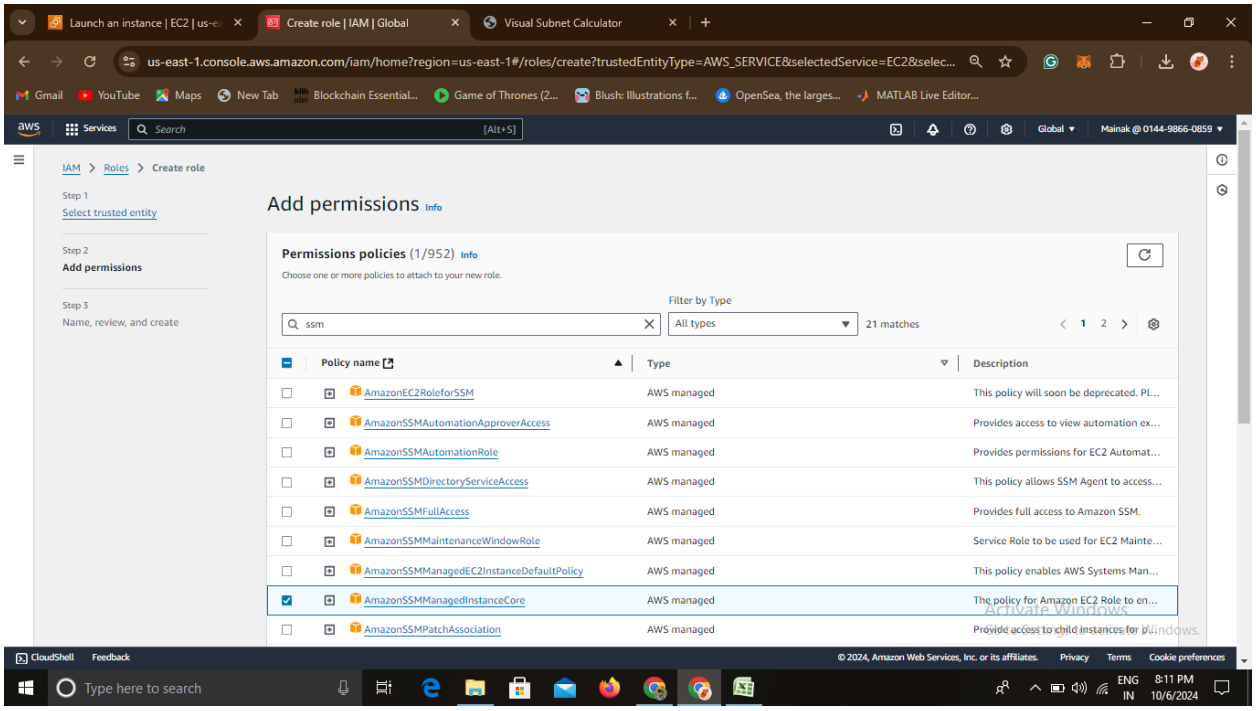


2.6 Create a Role for connection of EC2 to Systems Manager.

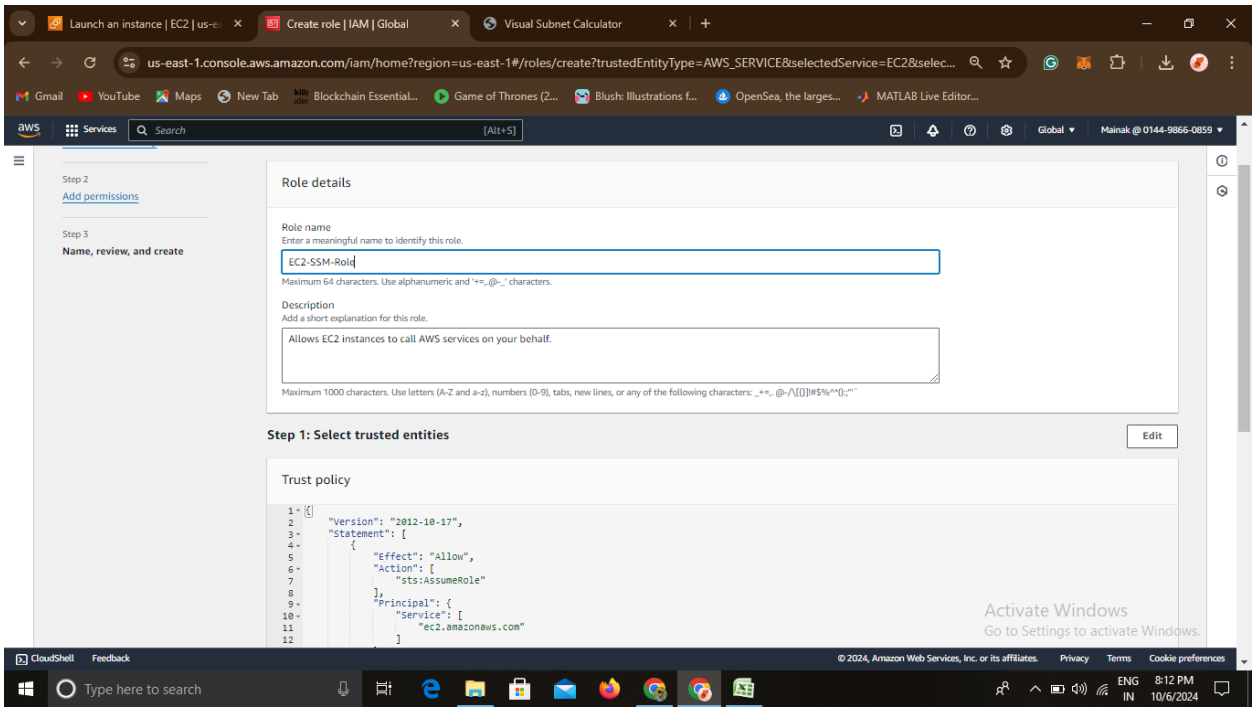




2.7 Assign the permissions policies



2.8 Enter the Role name and add the trust policy for so.


Launch an instance | EC2 | us-e
Create role | IAM | Global
Visual Subnet Calculator
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create?trustedEntityType=AWS_SERVICE&selectedService=EC2&selec...
Gmail
YouTube
Maps
New Tab
Blockchain Essential...
Game of Thrones (2...
Blush: Illustrations f...
OpenSea, the larges...
MATLAB Live Editor...
aws
Services
Search
[Alt+S]
Global
Mainak @ 0144-9866-0859
Step 2
Add permissions
Step 3
Name, review, and create
Role details
Role name
Enter a meaningful name to identify this role.
EC2-SSM-Role
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,. @-/\[{}]!#$%^*{};:"`
Step 1: Select trusted entities
Edit
Trust policy
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"sts:AssumeRole"
],
"Principal": {
"Service": [
"ec2.amazonaws.com"
]
Activate Windows
Go to Settings to activate Windows.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
IN
8:12 PM
10/6/2024

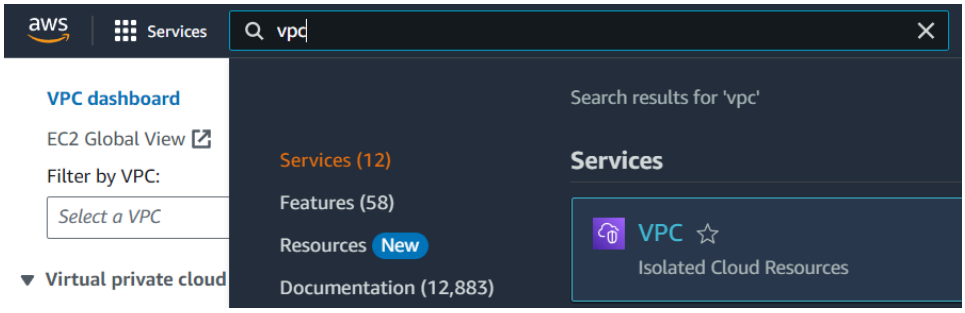
3. VPC Configuration

VPCs Configuration:

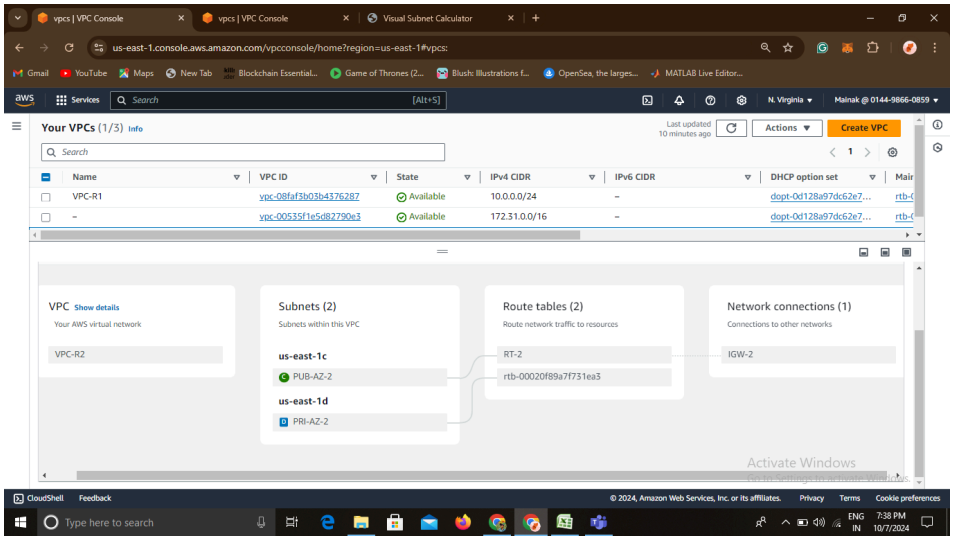
- In the VPC dashboard, click on Create VPC. Enter a name and add a IPv4 CIDR block of **10.0.0.0/24**. Then create 2 public and 2 private subnets in diff AZs.
- Create Internet Gateway and NAT Gateway and attach to VPC and associate the IG and NG in the Route Tables resp.
- Similarly create one more VPC of IPv4 CIDR block of **10.1.0.0/24** and configure it.

Step 3: Launch VPC in Console

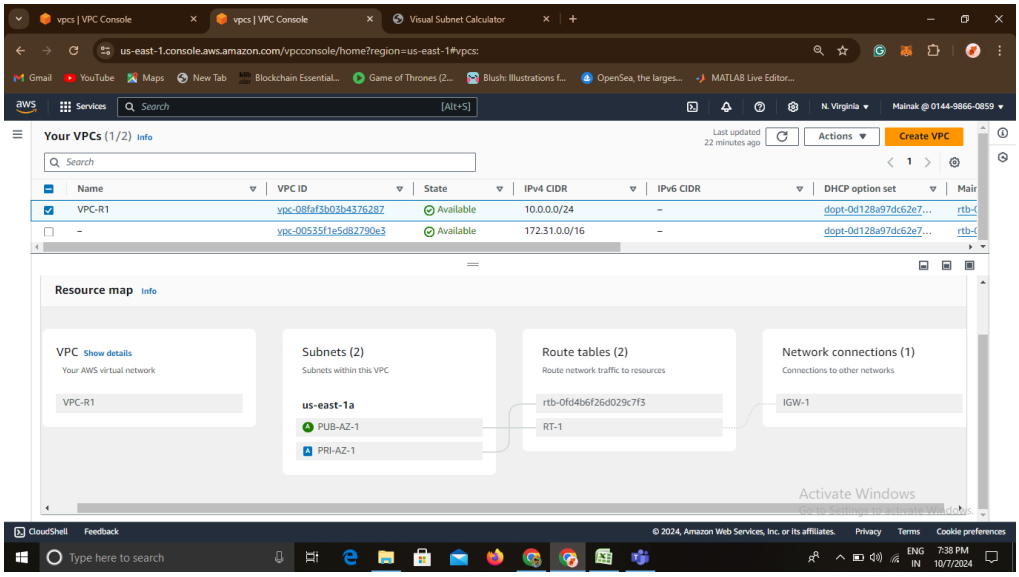
3.1 In Dashboard, search for VPC service, click **VPC** to open it.



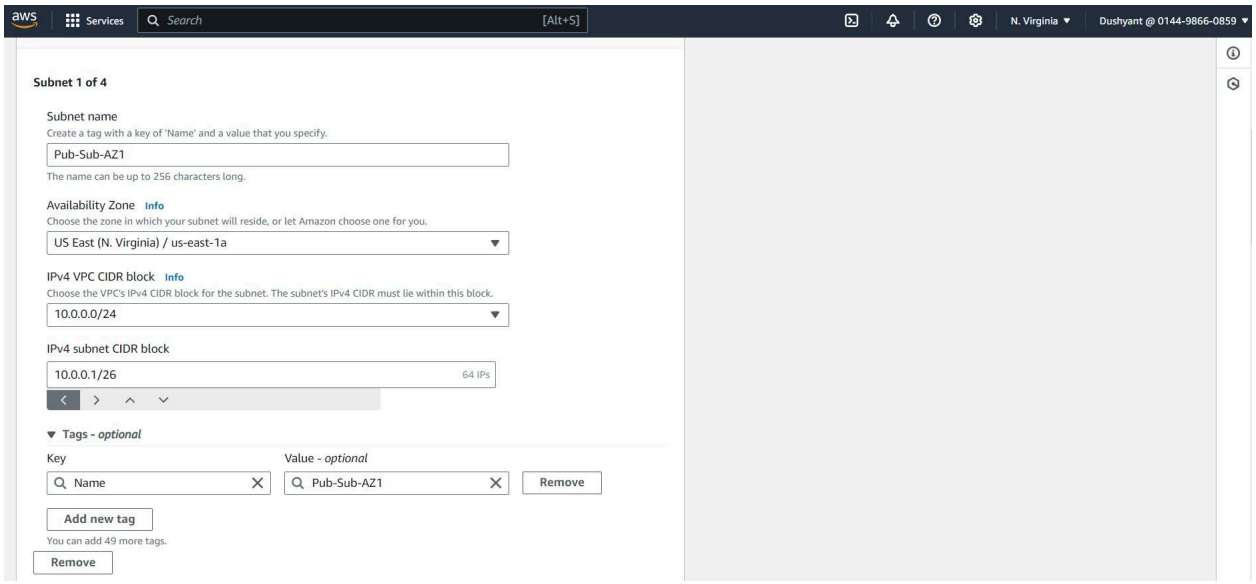
3.2 Click **Create VPC** to configure.

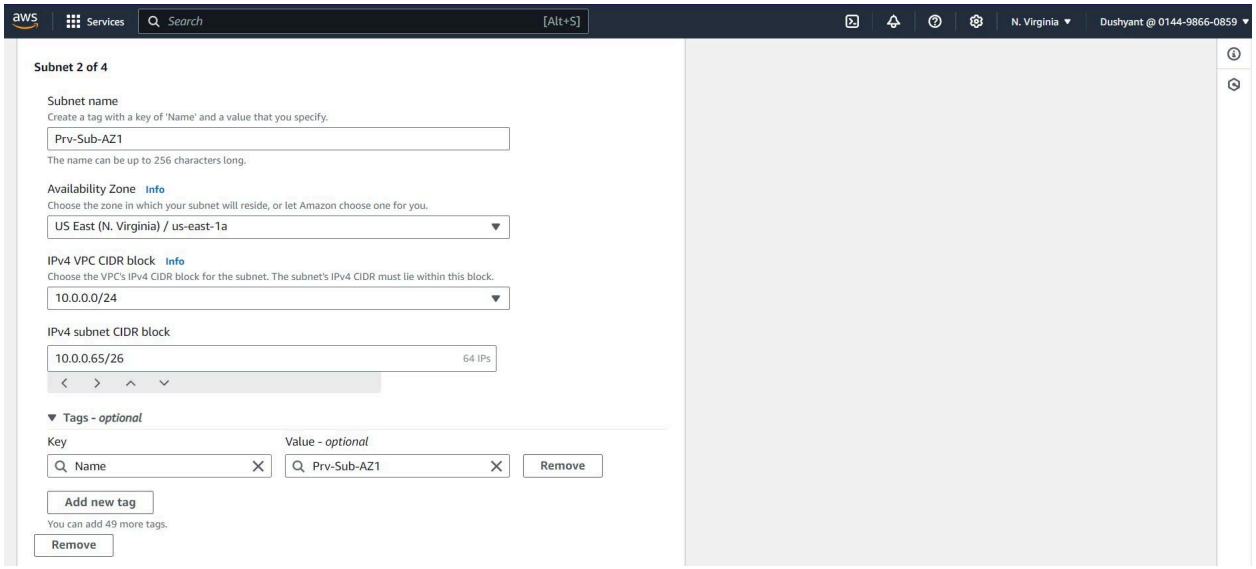


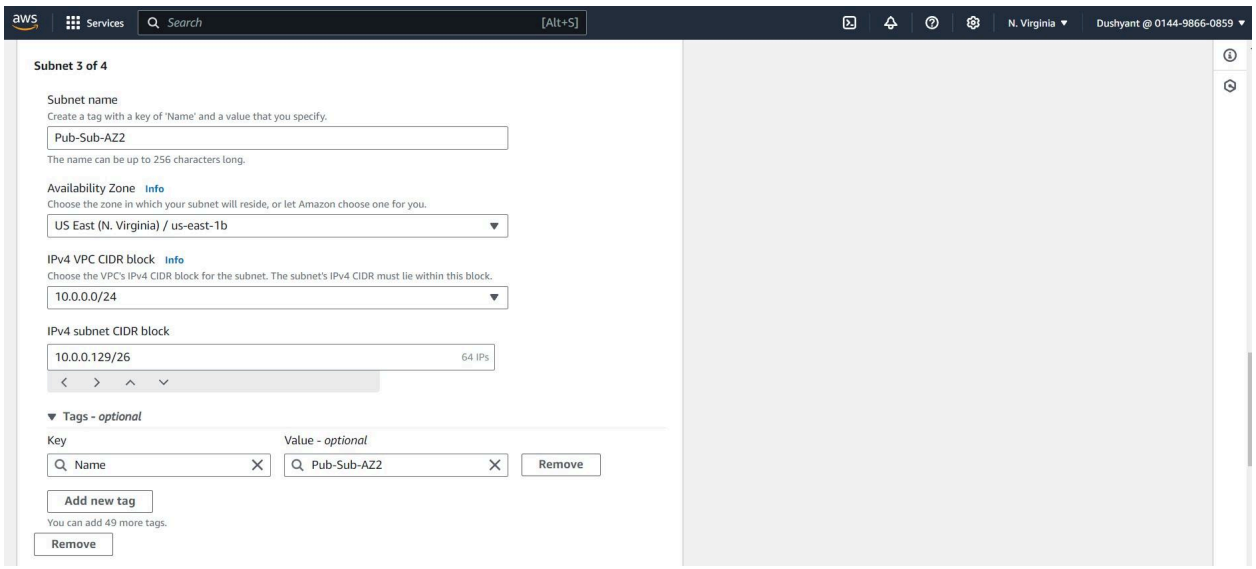
3.3 Type the **Name** which you prefer for naming the VPC and allocate the IPv4 CIDR block as **10.0.0.0/24**.

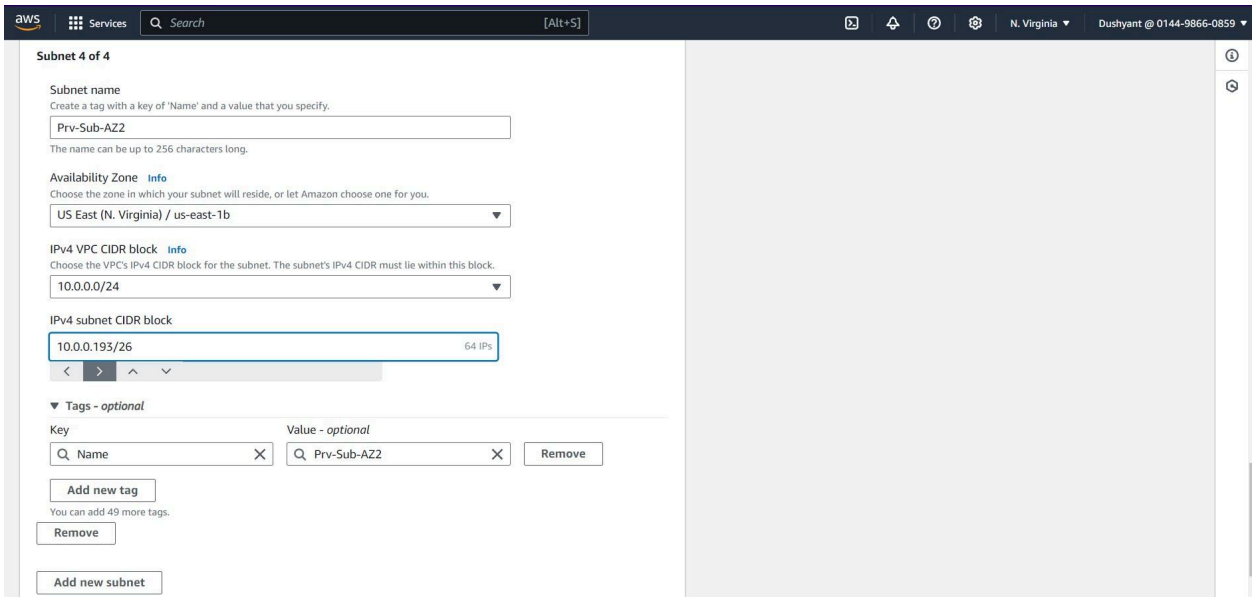


3.4 Now,select the subnets in the left pane and create **4 Subnets,** two Public for EC2 and other two Private for RDS with CIDR as **10.0.0.0/26, 10.0.0.128/26** and **10.0.0.64/26, 10.0.0.92/26** respectively.

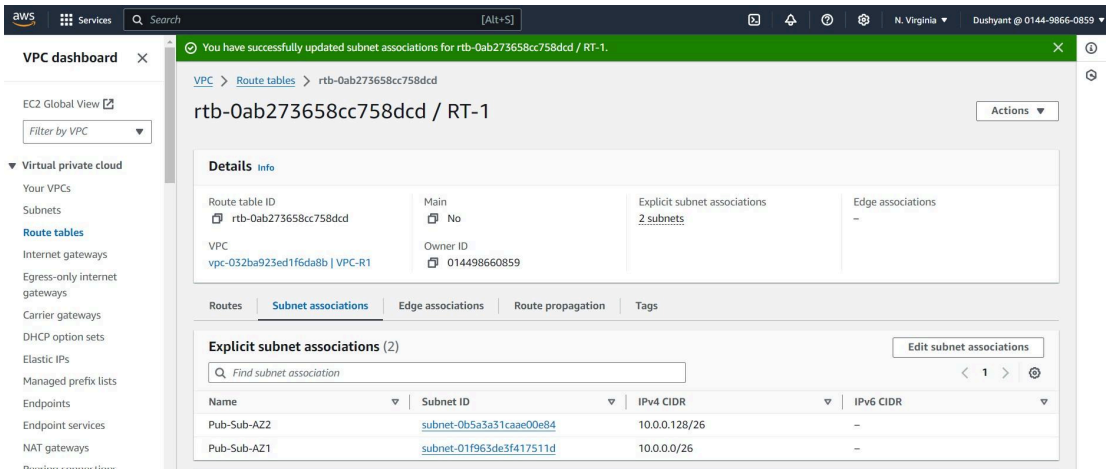

aws
Services
Search
[Alt+S]
N. Virginia
Dushyant @ 0144-9866-0859
Subnet 1 of 4
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Pub-Sub-AZ1
The name can be up to 256 characters long.
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1a
IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/24
IPv4 subnet CIDR block
10.0.0.1/26
64 IPs
Tags - optional
Key
Value - optional
Name
Pub-Sub-AZ1
Remove
Add new tag
You can add 49 more tags.
Remove

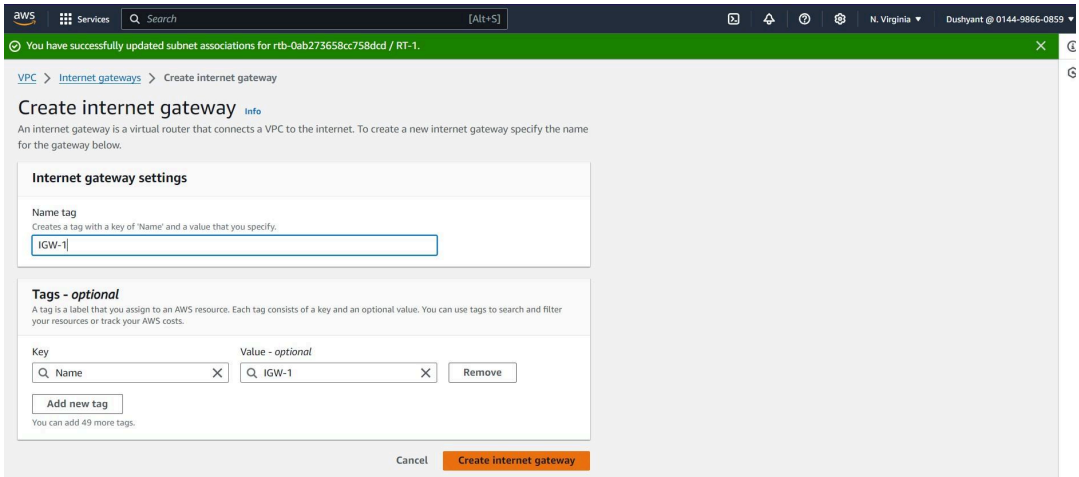

aws
Services
Search
[Alt+S]
N. Virginia
Dushyant @ 0144-9866-0859
Subnet 2 of 4
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Prv-Sub-AZ1
The name can be up to 256 characters long.
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1a
IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/24
IPv4 subnet CIDR block
10.0.0.65/26
64 IPs
Tags - optional
Key
Value - optional
Name
Prv-Sub-AZ1
Remove
Add new tag
You can add 49 more tags.
Remove

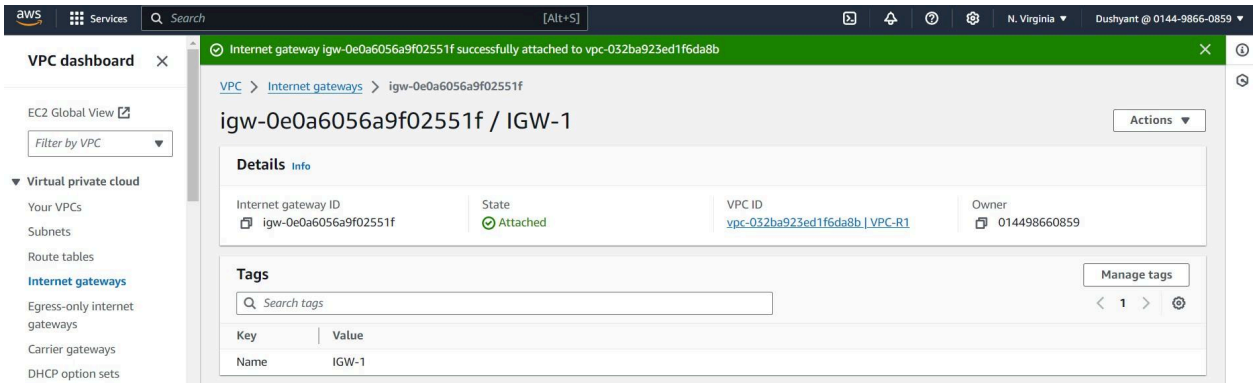

aws
Services
Search
[Alt+S]
N. Virginia
Dushyant @ 0144-9866-0859
Subnet 3 of 4
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Pub-Sub-AZ2
The name can be up to 256 characters long.
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1b
IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/24
IPv4 subnet CIDR block
10.0.0.129/26
64 IPs
Tags - optional
Key
Value - optional
Name
Pub-Sub-AZ2
Remove
Add new tag
You can add 49 more tags.
Remove

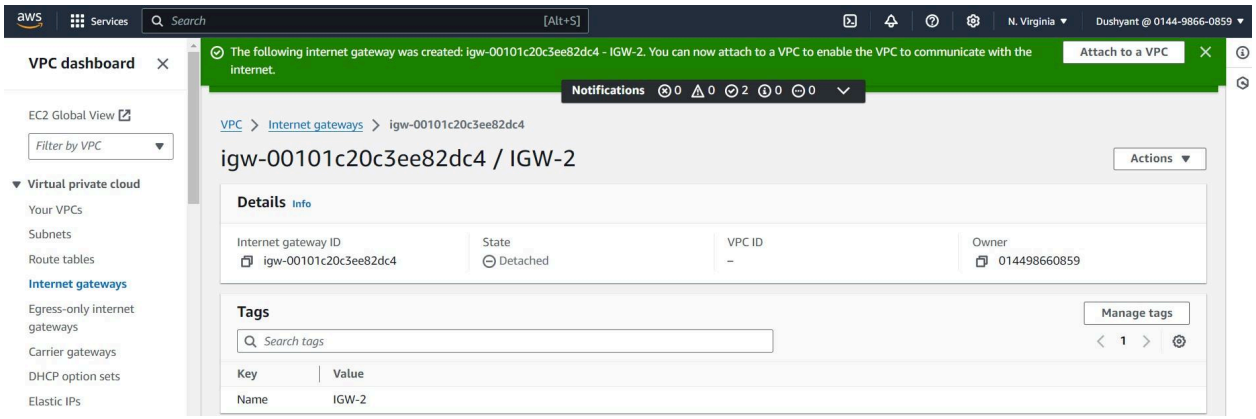


3.5 After creating the subnets now create an internet gateway, NAT gateway and Route table.

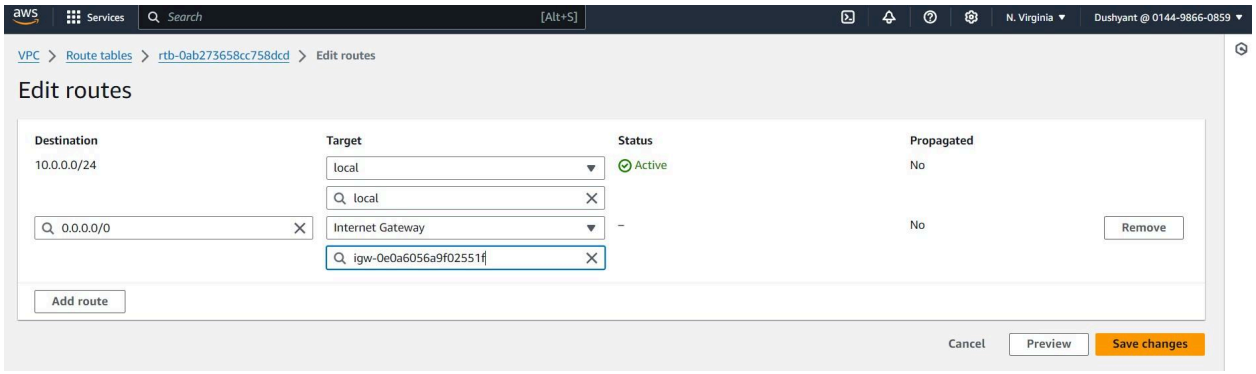


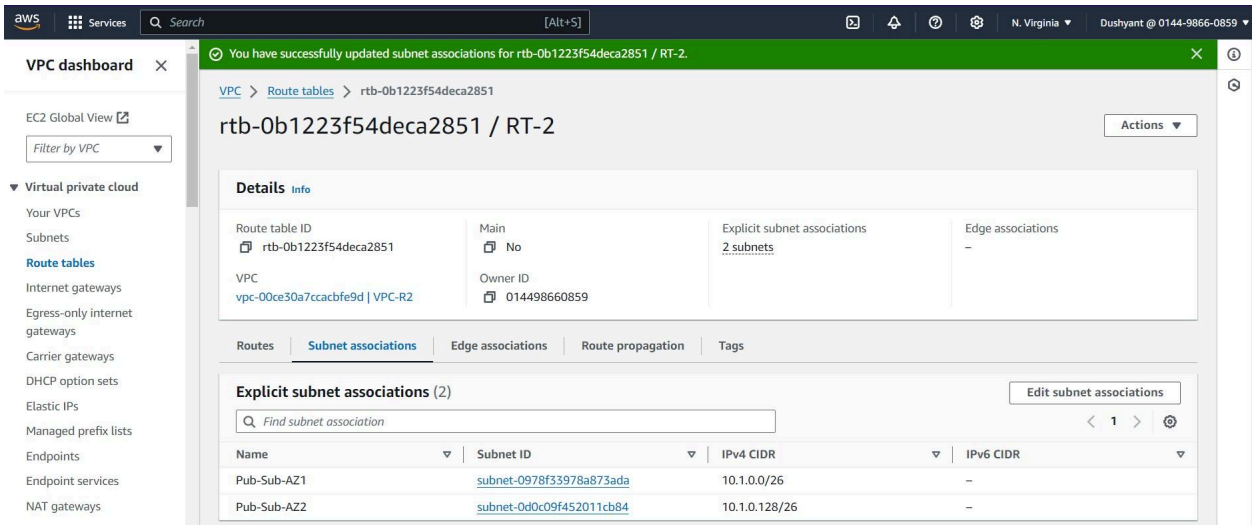




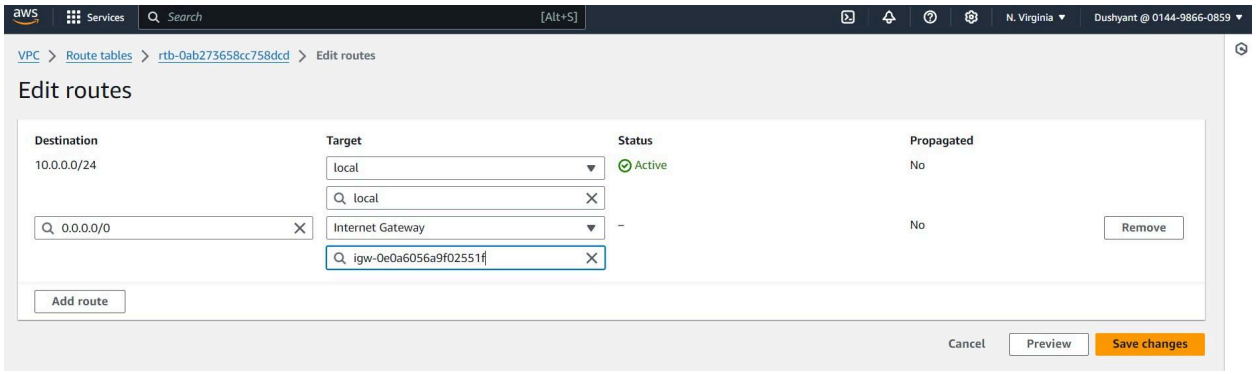


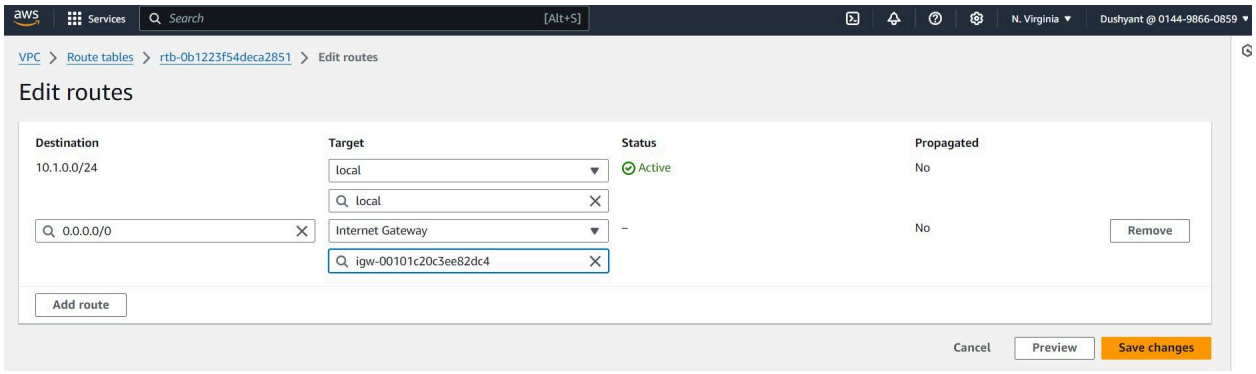
3.6 Under Route Tables created associate the subnets based upon the resource enlisted such as public or private subnets.



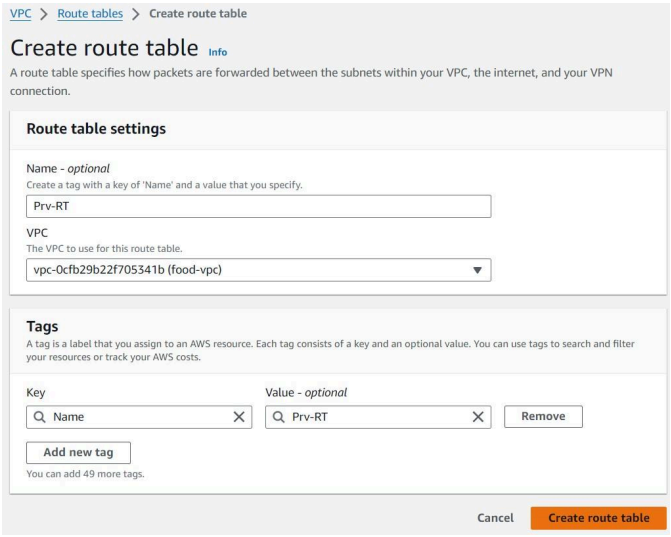


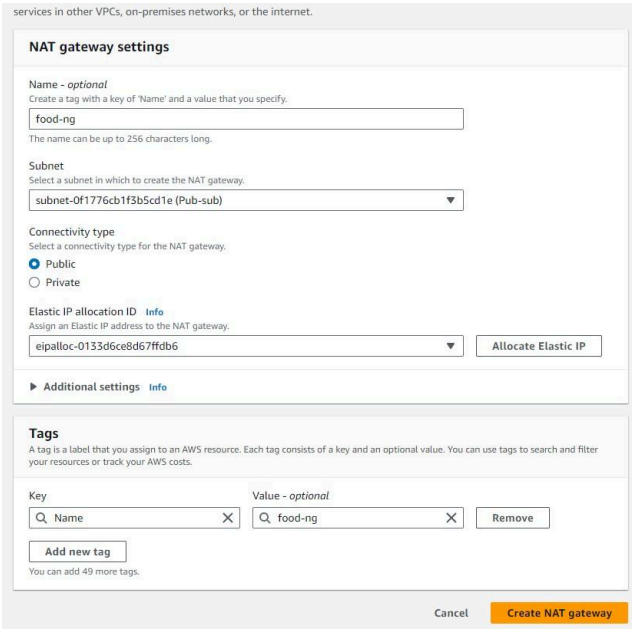
3.7 Attaching internet gateway for Public route table.

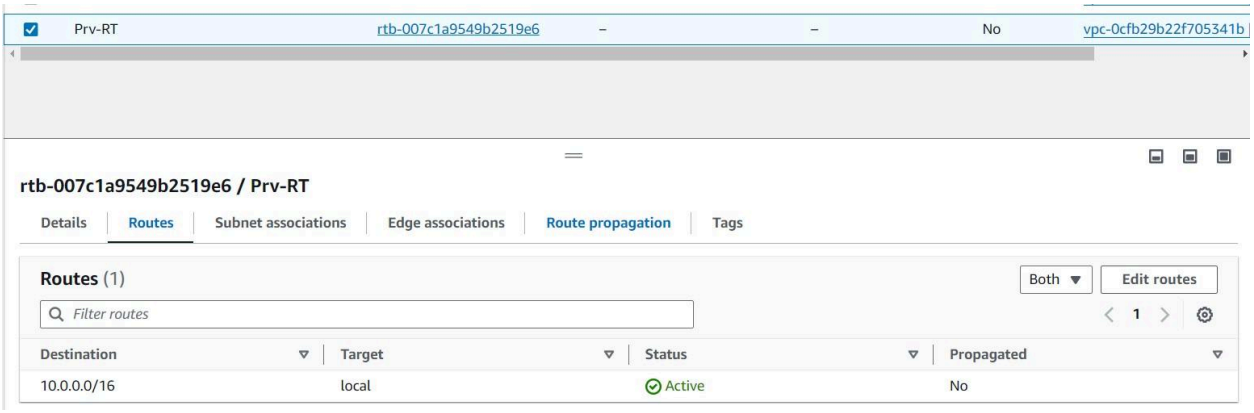




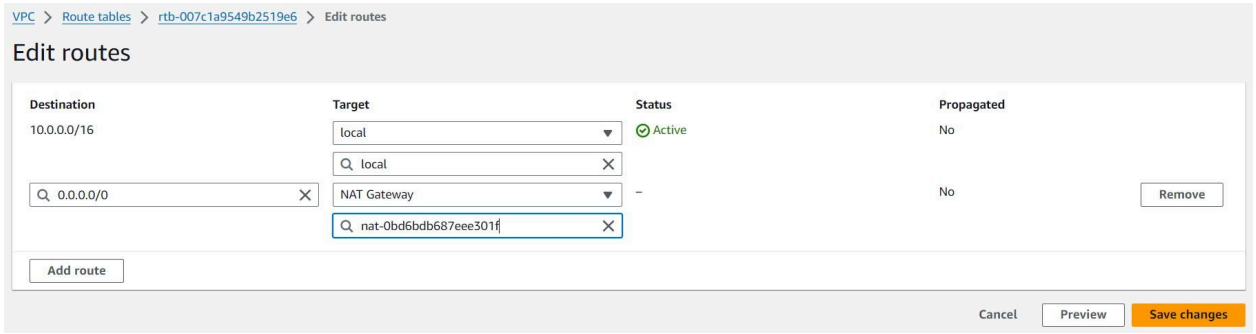
3.8 Similarly, create a route table for Private and allocate the nat gateway and association of it.



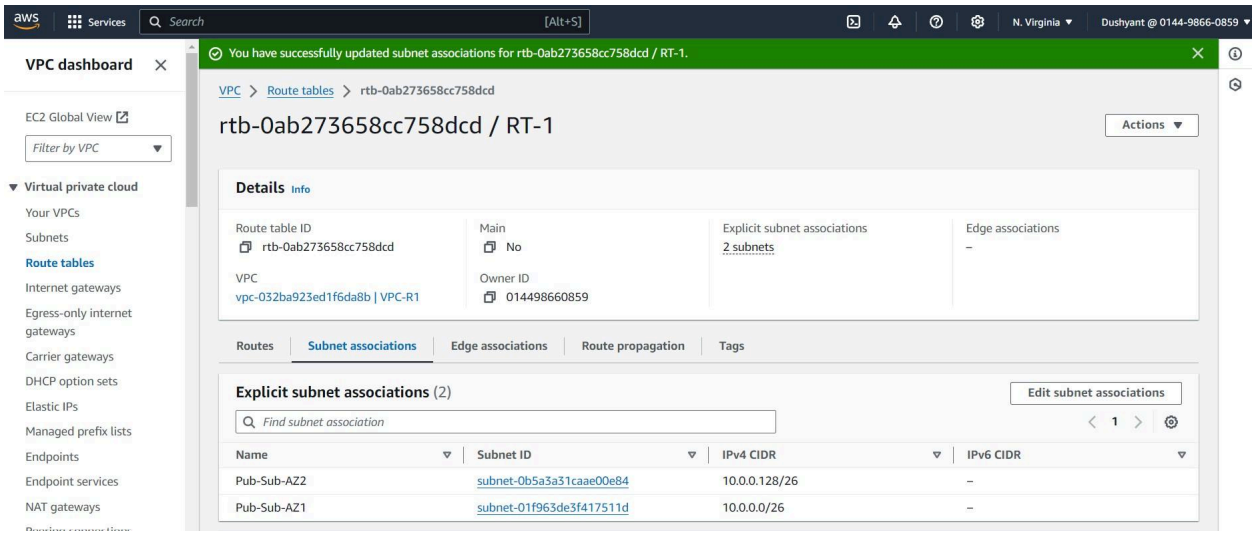


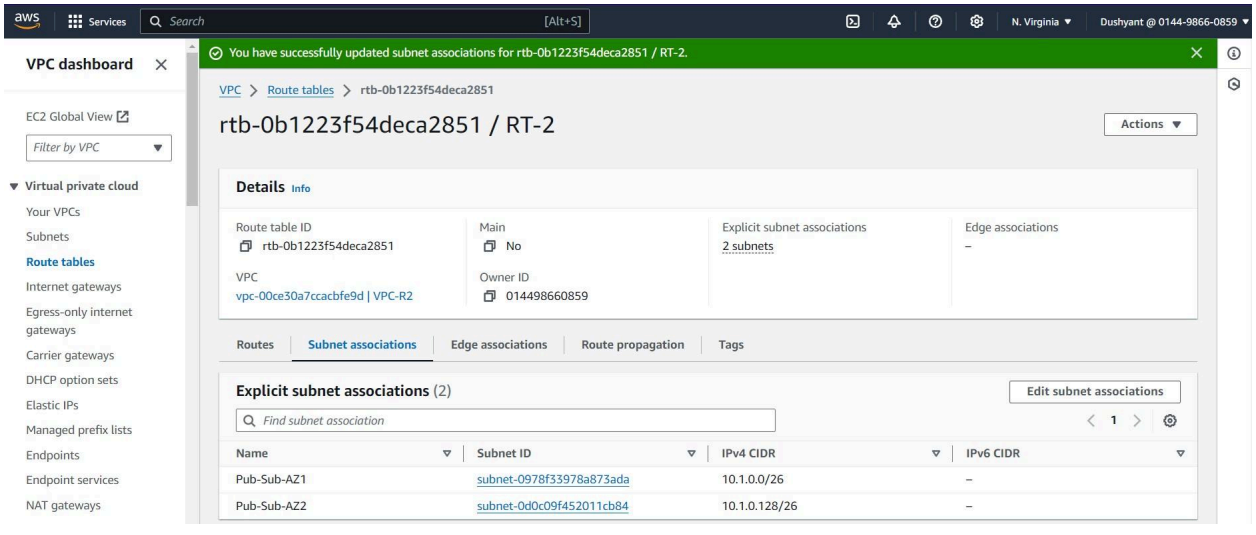


3.9 After creating the route table, add a route to allow Internet access.



3.10 Now we will associate subnets with Route Tables.





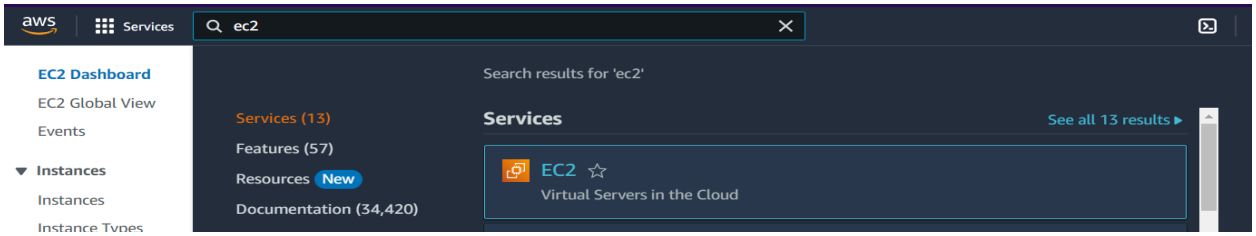
4. EC2 Configuration

EC2s Configuration:

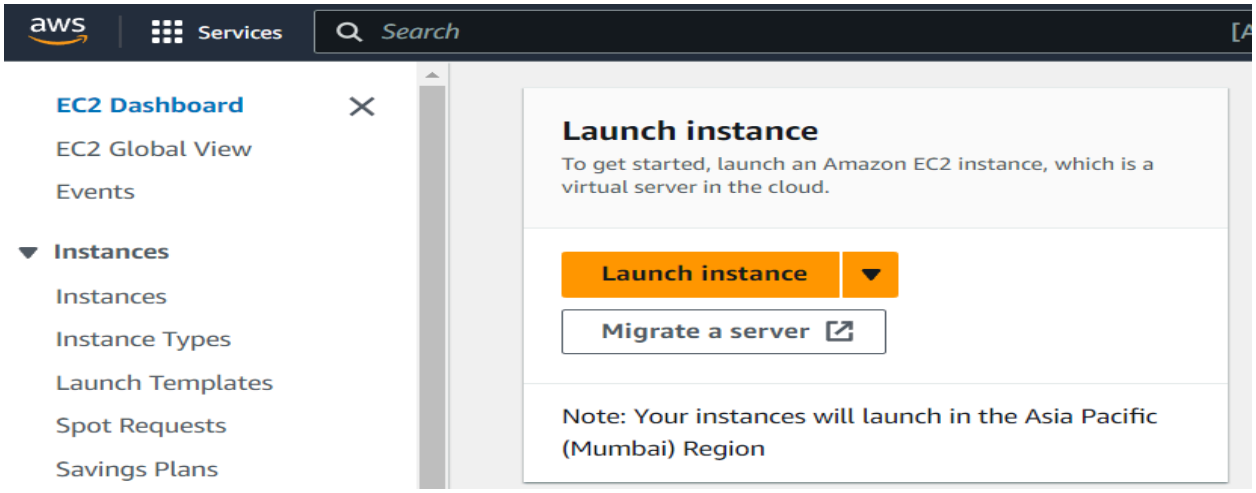
- In the EC2 dashboard, click on **Launch Instance**.
- On the **Choose an Amazon Machine Image (AMI)** page, click on the **AWS Marketplace** tab.
- Browse through the available AMIs and search for CentOS 9 Desktop - GUI Gnome with RDP by Arara Solutions.
- Configure the Instance details, network, storage and security group and attach the EC2-Systems Manager Role and launch the instance.

Step 4: Launch EC2 in Console

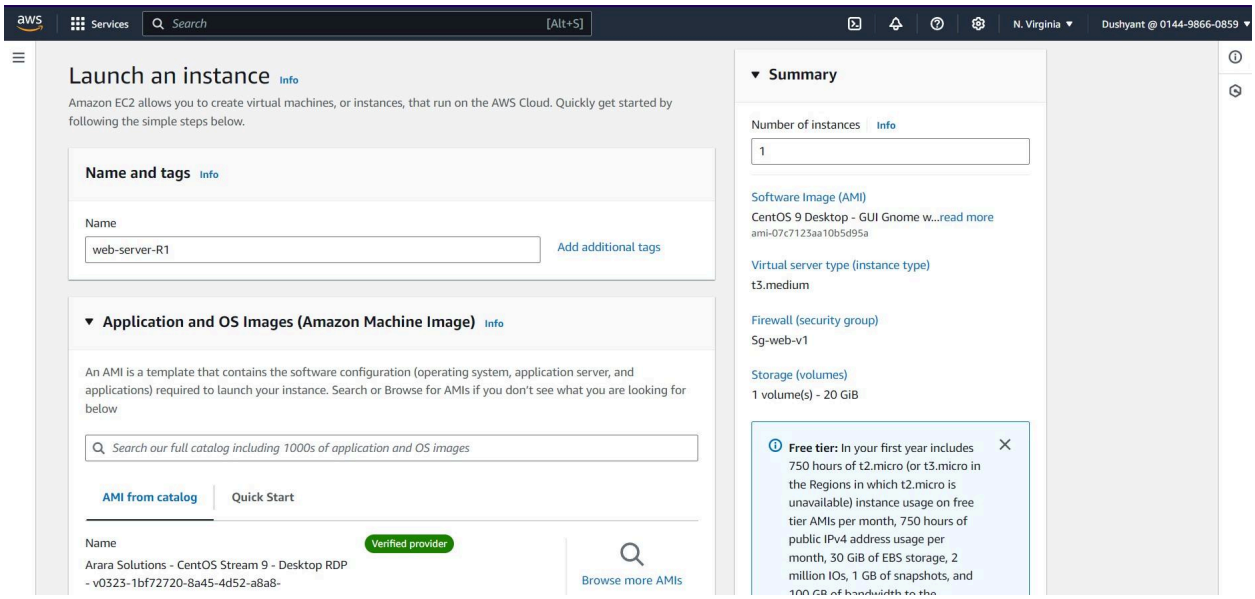
4.1 In Dashboard, search for EC2 service, click **EC2** to open it.



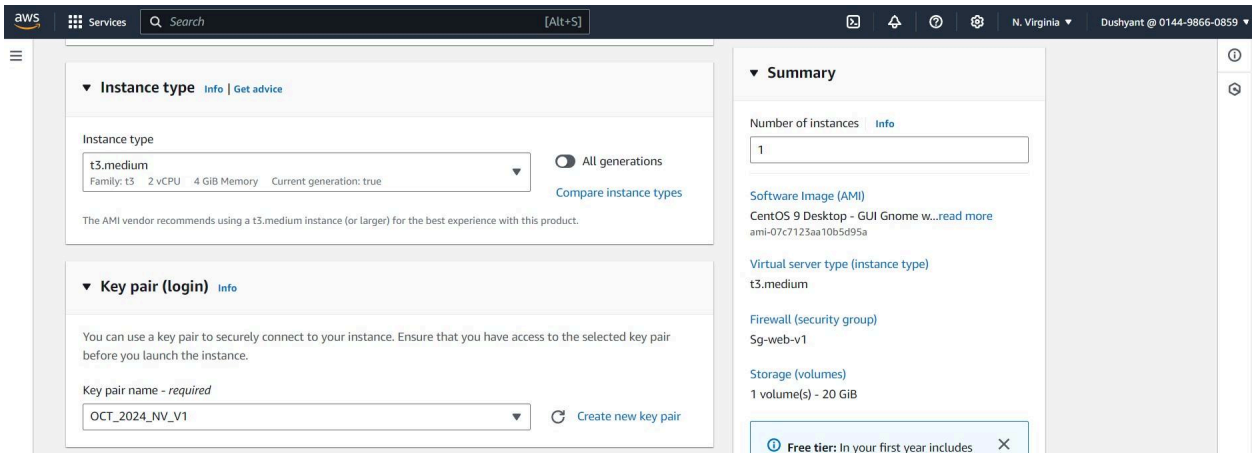
4.2 Click **Launch instance** to configure.

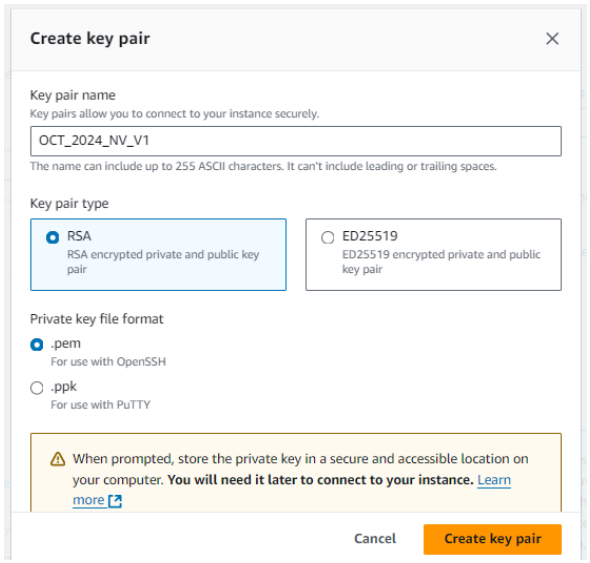


4.3 Type the **Name** which you prefer for naming the instance and Choose the **AMI**, so here we are using **CentOS**.

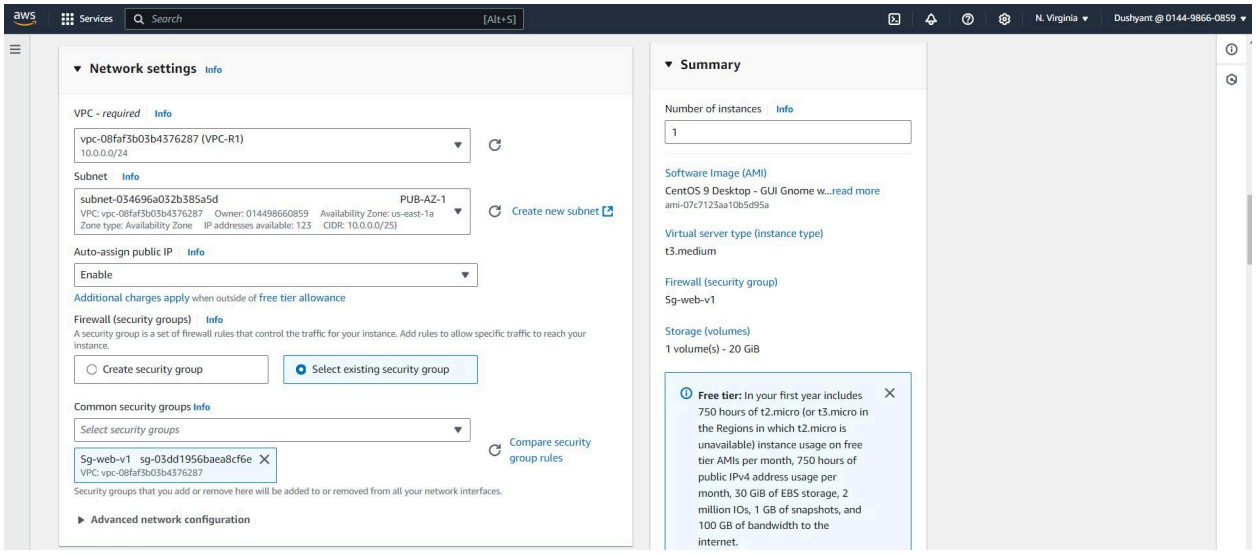


4.4 Select the instance type **t2.micro** and then create the pair to do that click on **Create new pair key** for secure connection.

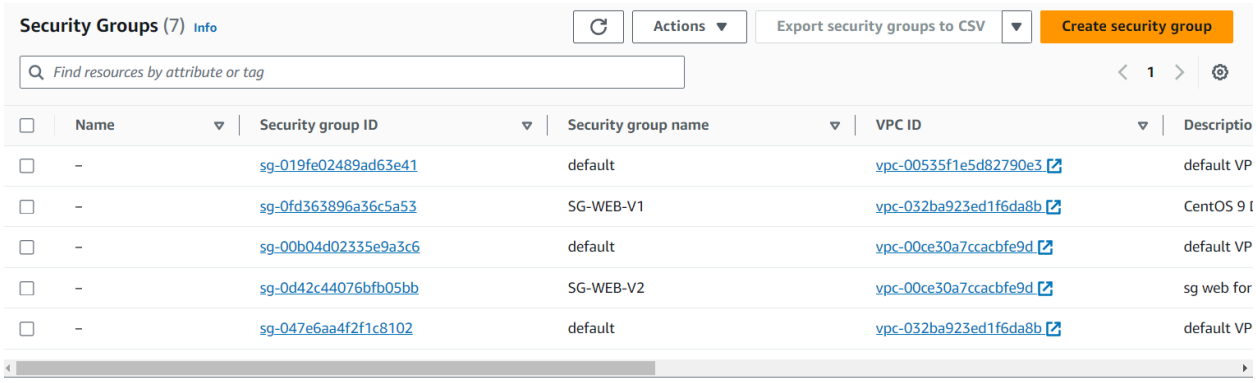


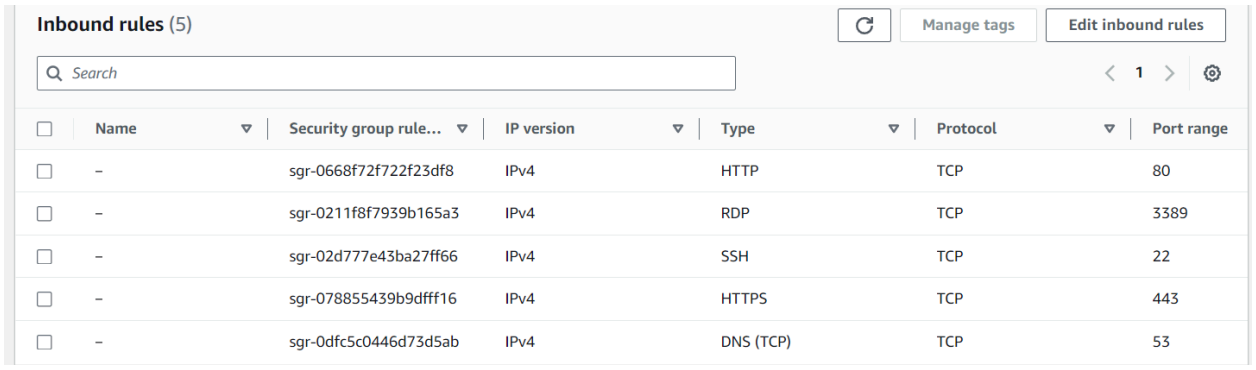


4.5 Under Network Settings, click **Edit** and under Firewall (security groups) choose **Create security group** option and then check in inbound security group rules that Type field is **HTTP** and source type field is **Anywhere**. If the above fields are not present then click **Add security group rule** and click those options.

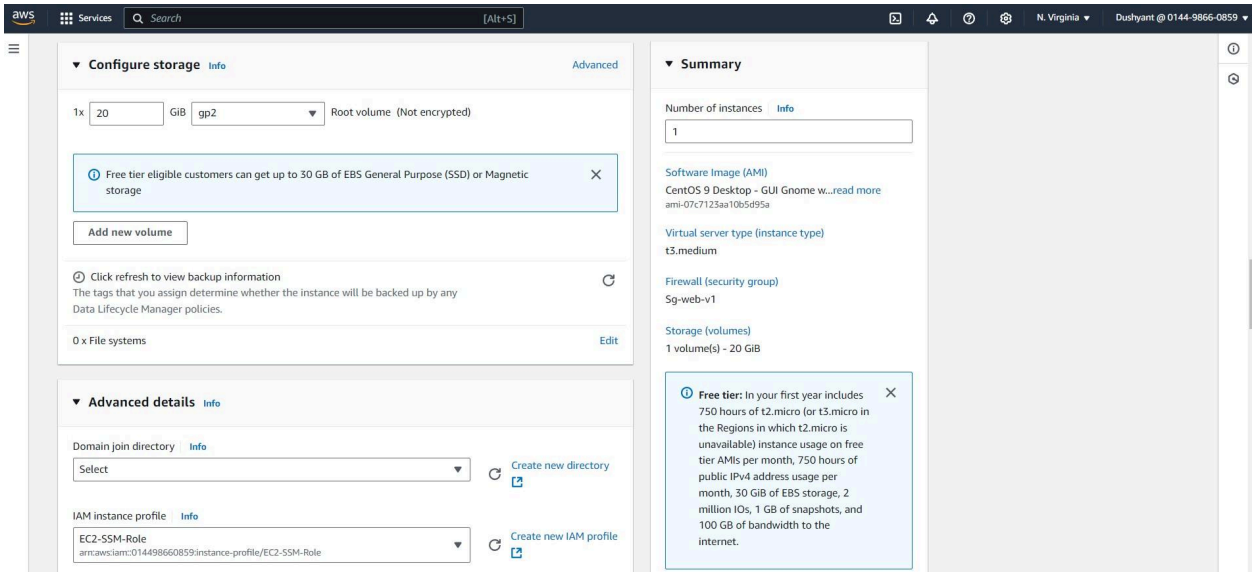


4.6 Configure Security Group.

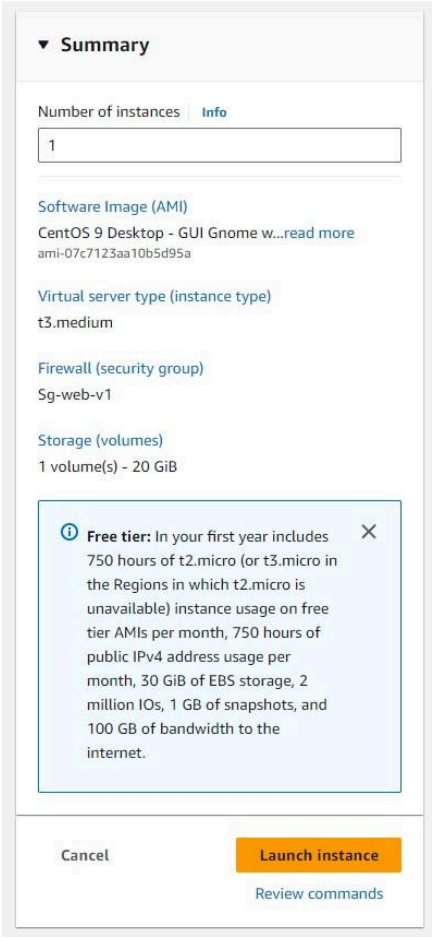




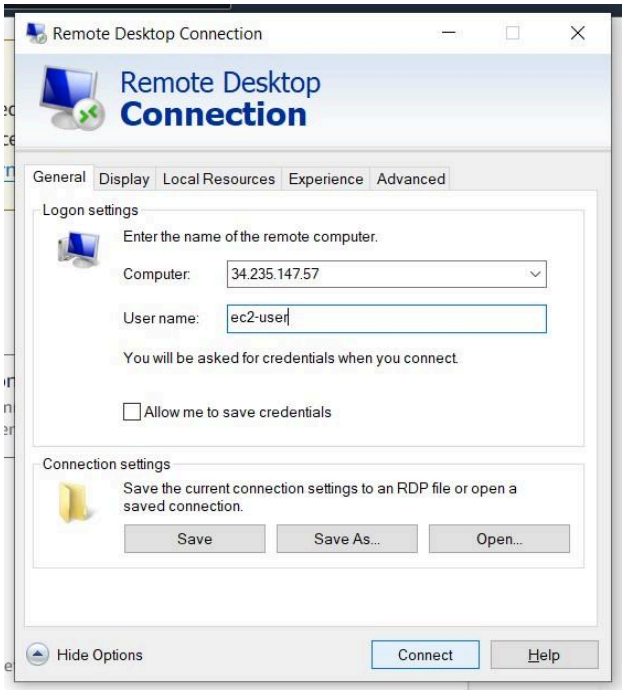
4.7 Go to the Advanced Details and under IAM instance profile allocate the role of EC2-SSM Role.

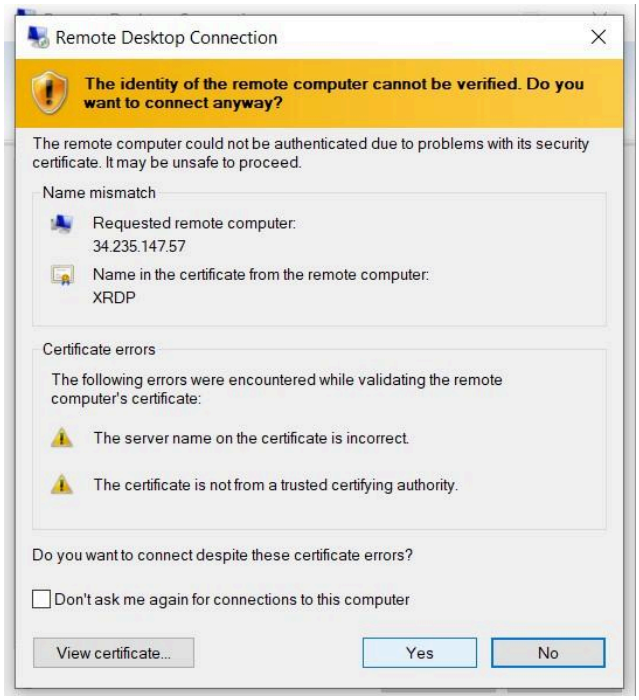


4.8 Leave rest configuration as default will come back later. Click on **Launch Instance**.

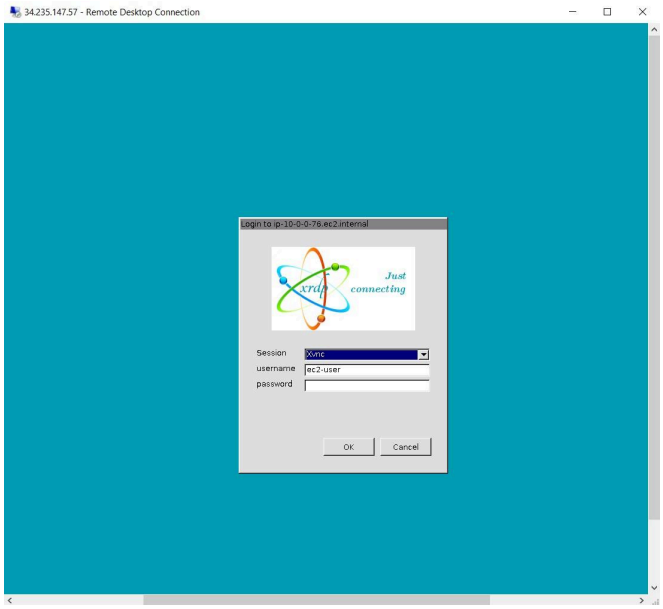


4.9 Using RDP to access an EC2 instance remotely.

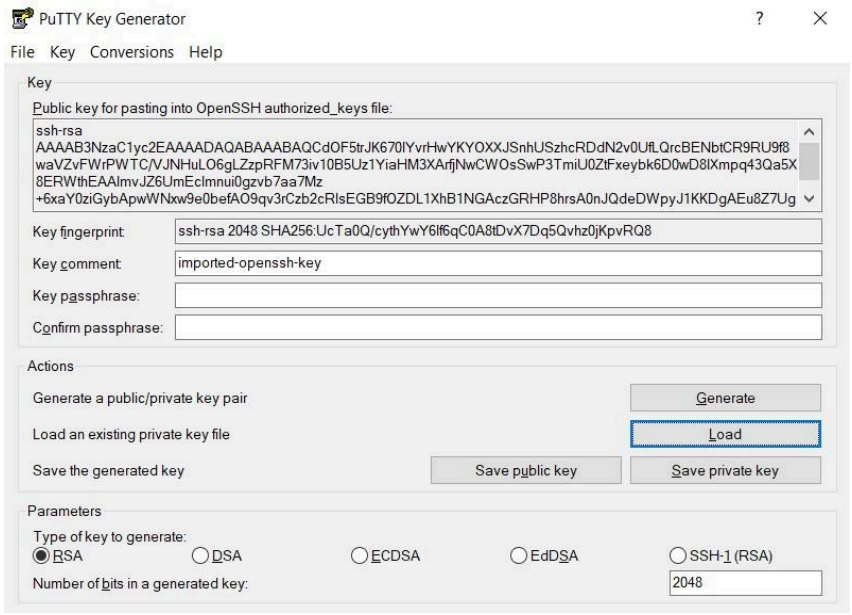




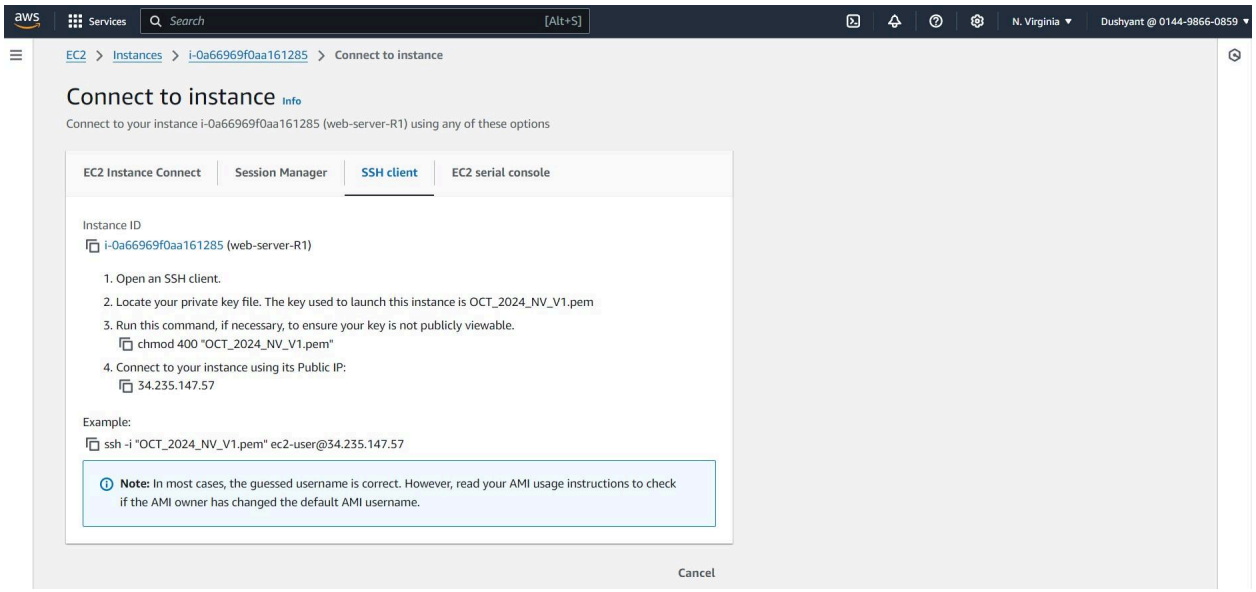
4.10 To login the XRDP CentOS GUI first have to setup the password.

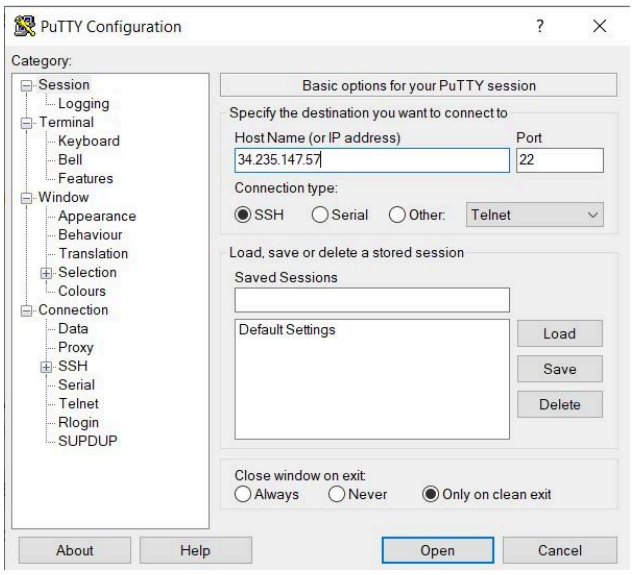


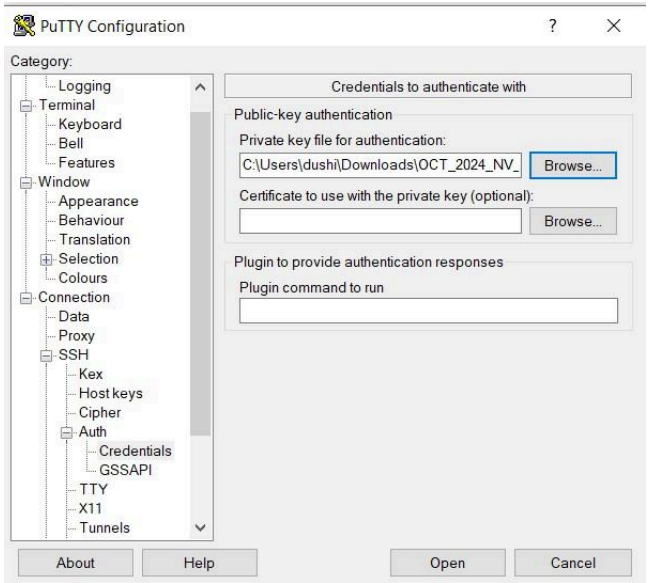
4.11 Convert the .pem file to .ppk file in puttygen



4.12 Using Putty to access an EC2 instance remotely.

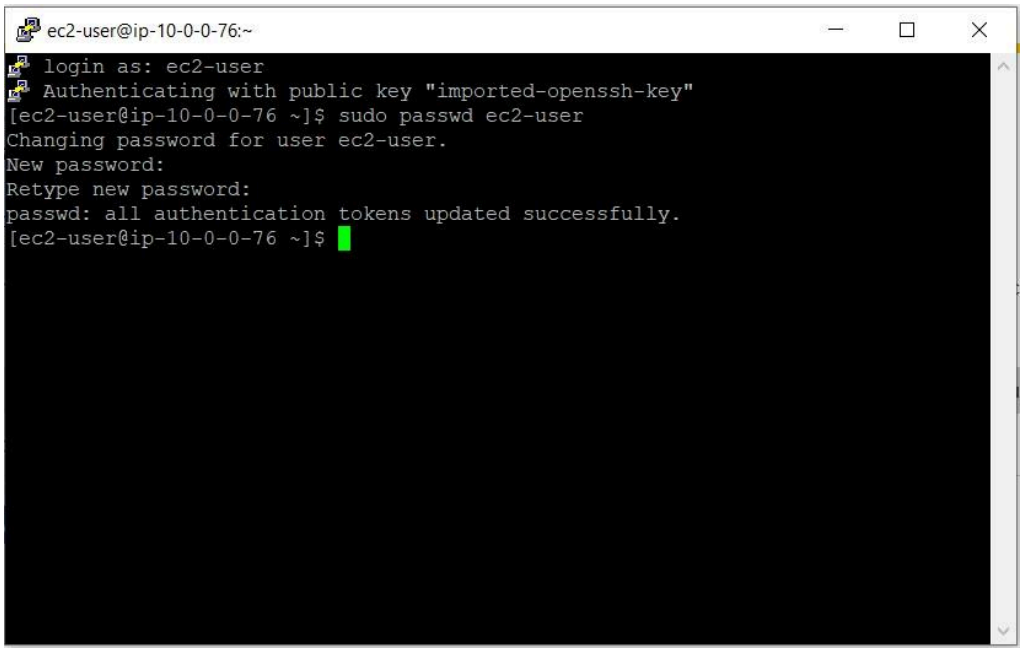

aws
Services
Search
[Alt+S]
N. Virginia
Dushyant @ 0144-9866-0859
EC2 > Instances > i-0a66969f0aa161285 > Connect to instance
Connect to instance Info
Connect to your instance i-0a66969f0aa161285 (web-server-R1) using any of these options
EC2 Instance Connect
Session Manager
SSH client
EC2 serial console
Instance ID
i-0a66969f0aa161285 (web-server-R1)
1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is OCT_2024_NV_V1.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
chmod 400 "OCT_2024_NV_V1.pem"
4. Connect to your instance using its Public IP:
34.235.147.57
Example:
ssh -i "OCT_2024_NV_V1.pem" ec2-user@34.235.147.57
Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.
Cancel


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Serial
Telnet
Rlogin
SUPDUP
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
34.235.147.57
22
Connection type:
SSH
Serial
Other:
Telnet
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel

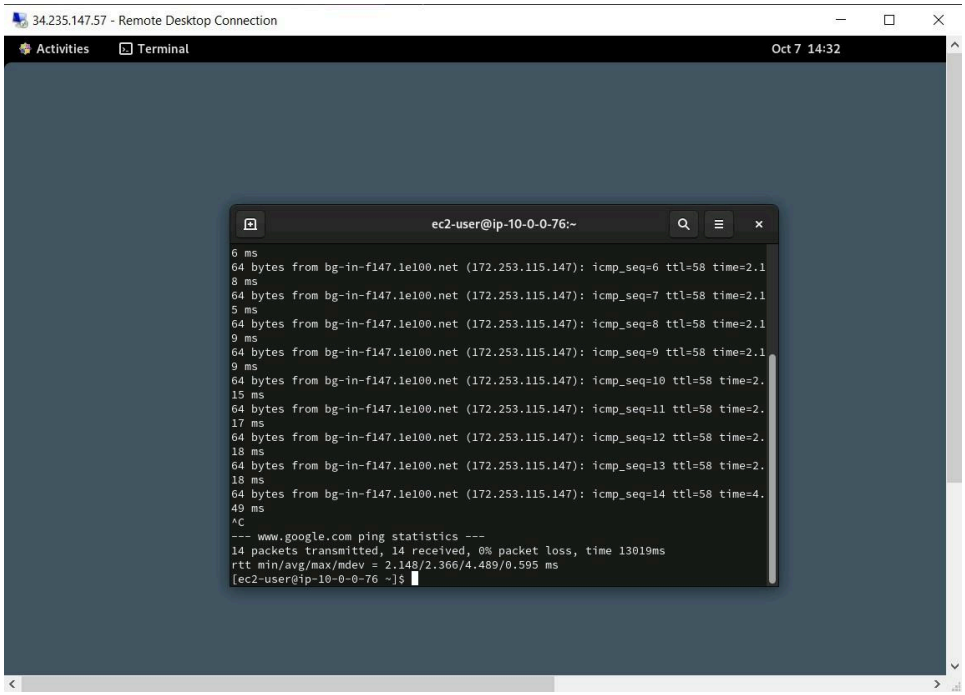

PuTTY Configuration
Category:
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Kex
Host keys
Cipher
Auth
Credentials
GSSAPI
TTY
X11
Tunnels
Credentials to authenticate with
Public-key authentication
Private key file for authentication:
C:\Users\dushi\Downloads\OCT_2024_NV_
Browse...
Certificate to use with the private key (optional):
Browse...
Plugin to provide authentication responses
Plugin command to run
About
Help
Open
Cancel

4.13 Assign the password by typing the command

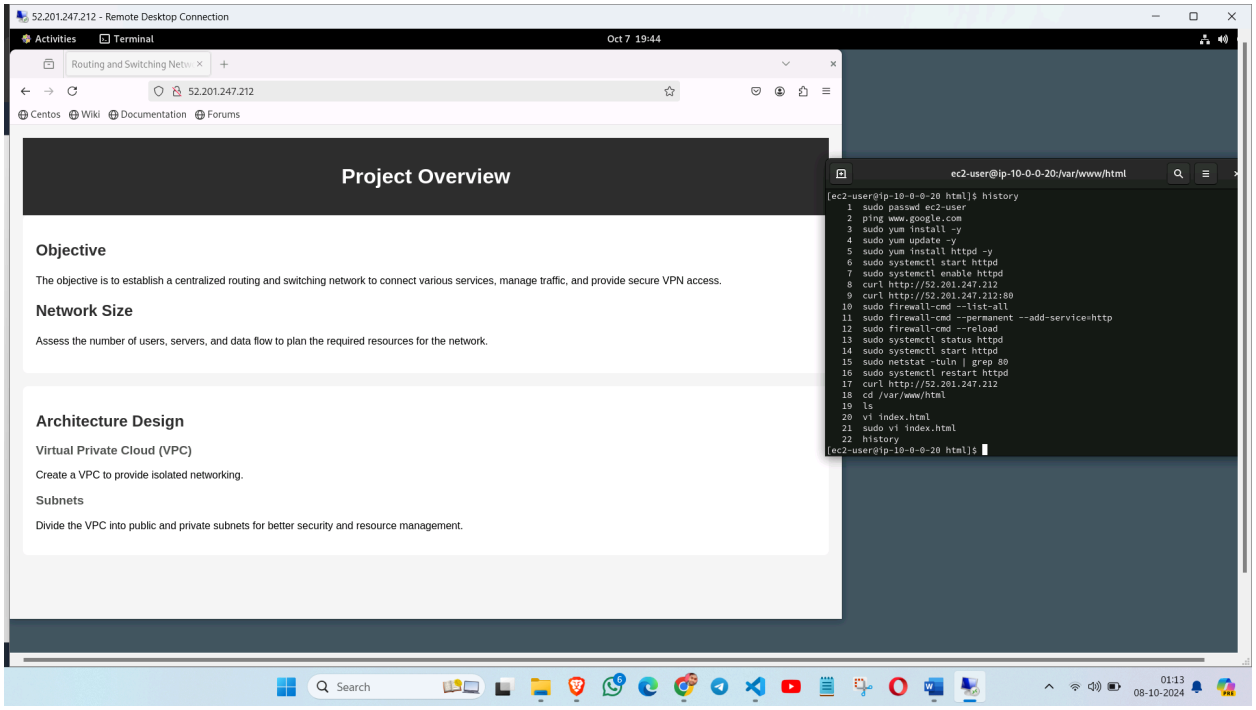
```
sudo passwd ec2-user
```



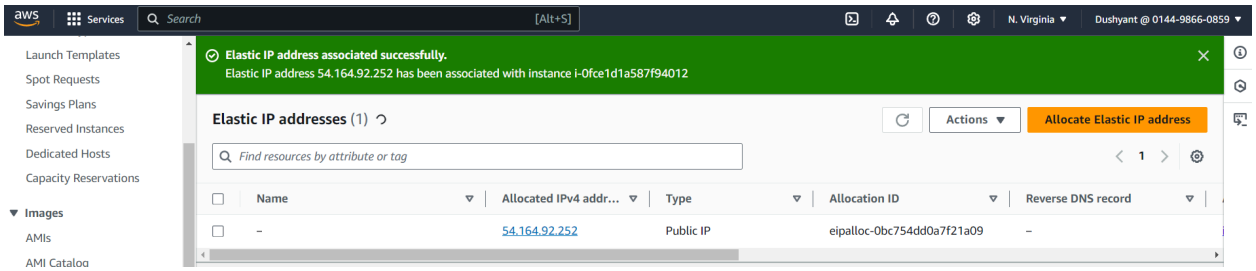
4.14 Finally, the CentOS GUI is launched and running.



4.15 Now launch the instances and configure the web server for adding the HTML files.



4.16 Create an Elastic IP and associate the EC2 instance.



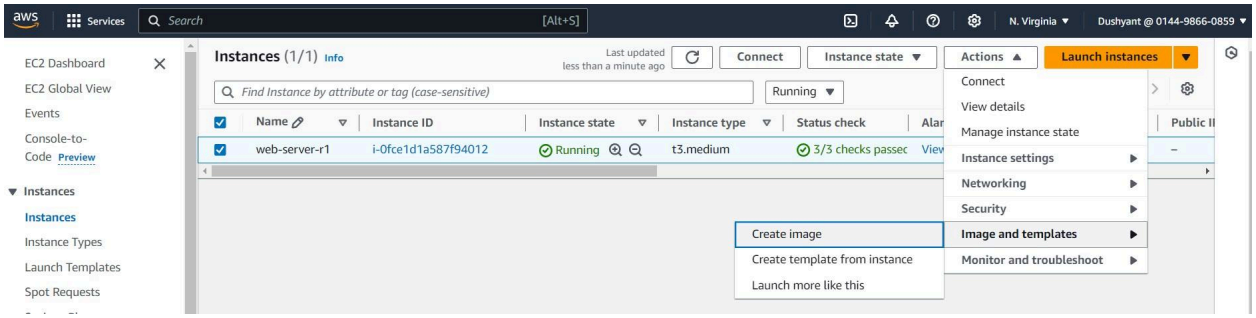
5. AMI Configuration

AMI Configuration:

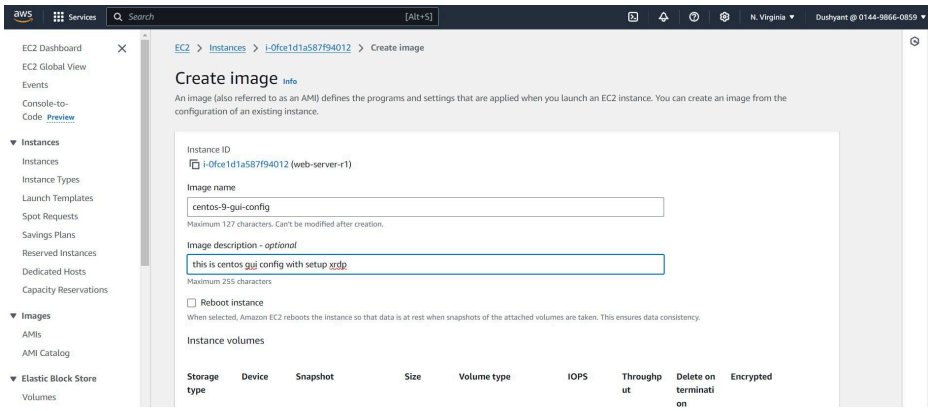
- Go to build Instance, click on **Actions** navigate to Image and Templates.
- Click Create Image and assign a name, check the description and disable the reboot checkbox and click Create Image
- Now, with the help of AMI, launch the other 3 EC2 instances and configure it.

Step 5: Build AMI from configured EC2 instance

5.1 In Dashboard, go to the Instances click on Actions and select Image and templates and Create Image.



5.2 Configure the description and disable the reboot checkbox.



EC2 > AMIs > ami-0fcb95d4393026a23

Image summary for ami-0fcb95d4393026a23

EC2 Image Builder | Actions | Launch instance from AMI

AMI ID ami-0fcb95d4393026a23	Image type machine	Platform details Linux/UNIX	Root device type EBS
AMI name centos-9-gui-config	Owner account ID 014498660859	Architecture x86_64	Usage operation RunInstances
Root device name /dev/sda1	Status Available	Source 014498660859/centos-9-gui-config	Virtualization type hvm
Boot mode –	State reason –	Creation date Mon Oct 07 2024 21:12:37 GMT+0530 (India Standard Time)	Kernel ID –
Description this is centos gui config with setup xrdp	Product codes marketplace:1nlootr6yyt4cdqma9d8ldy5e	RAM disk ID –	Deprecation time –
Last launched time Tue Oct 08 2024 00:07:25 GMT+0530 (India Standard Time)	Block devices /dev/sda1=snap-00966d3aa24356213:20:true:gp2	Deregistration protection Disabled	

Amazon Machine Images (AMIs) (1) Info

Recycle Bin | EC2 Image Builder | Actions | Launch instance from AMI

Owned by me | Find AMI by attribute or tag | 1

Name	AMI name	AMI ID	Source	Owner	Visibility
	centos-9-gui-config	ami-0fcb95d4393026a23	014498660859/centos-9-gui-config	014498660859	Private

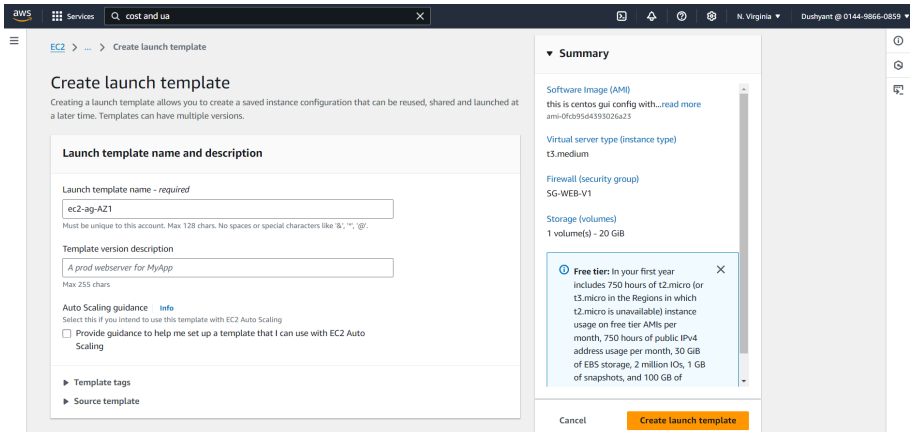
6. Auto Scaling Configuration

Auto Scaling Configuration:

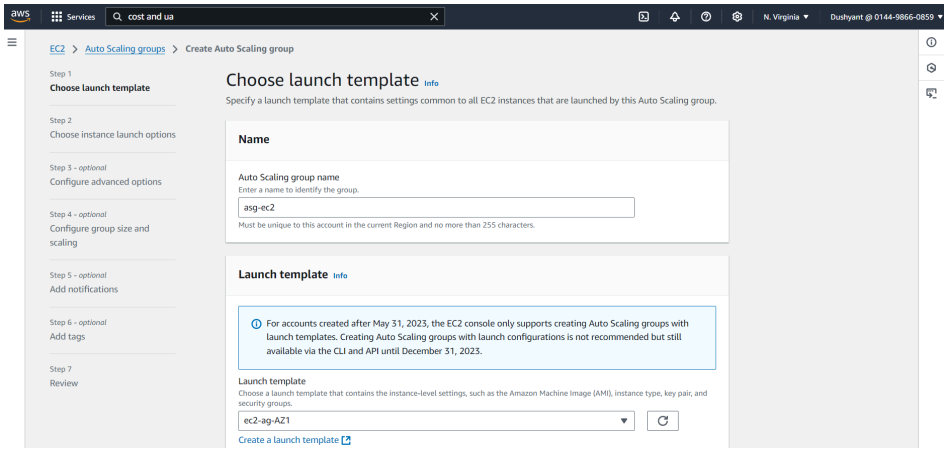
- In the EC2 dashboard, click on **Launch Templates**, assign the name and instance type and click **Create launch template.**
- Now, click **Create Auto Scaling group** and select the VPC and subnets.
- Configure the group size and scaling policies and click Create Auto Scaling Group.

Step 6: Build Launch Template to configure Auto Scaling instances

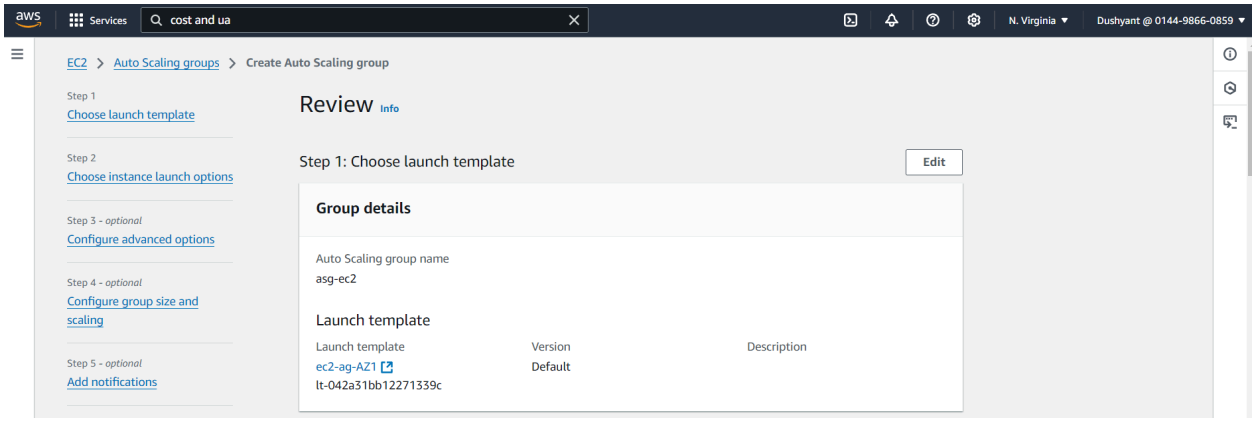
6.1 Build a launch template from the AMI we have created.

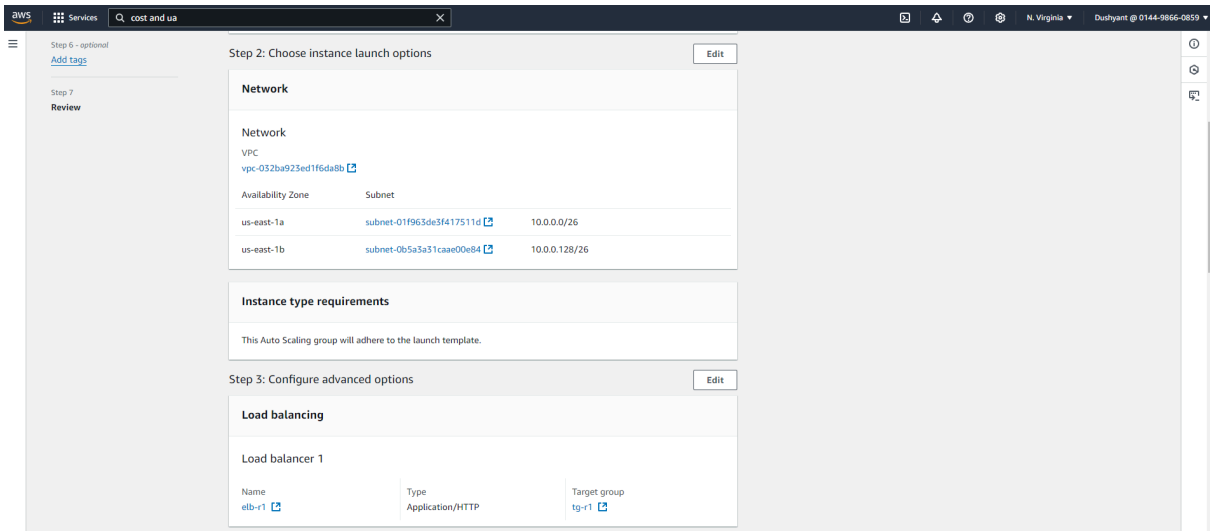


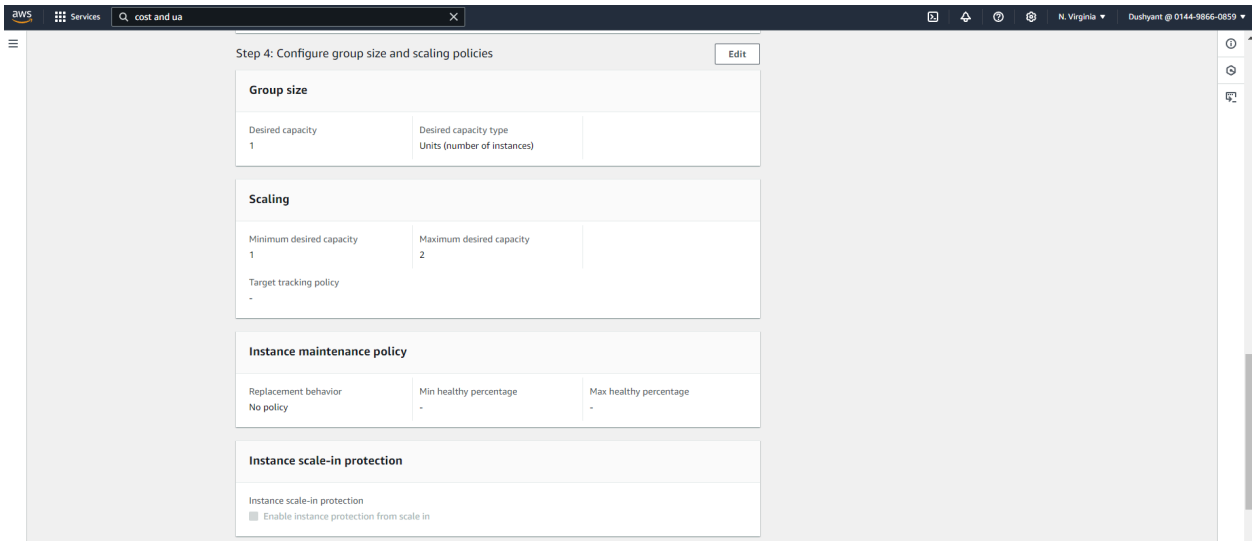
6.2 Now, create the auto scaling group and attach the launch template.



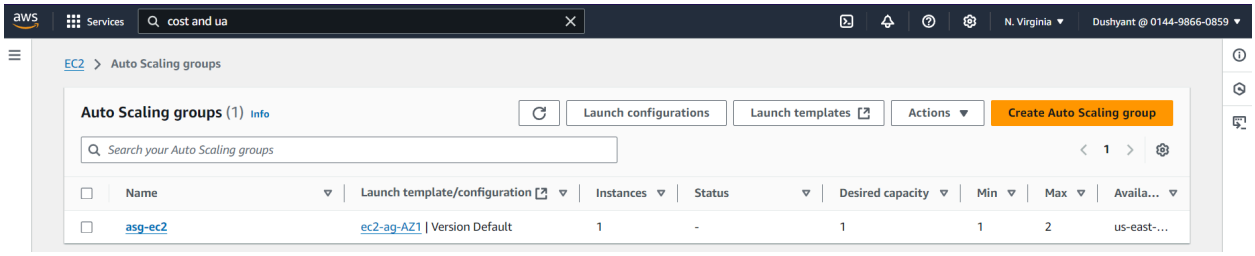
6.3 Configure it and review the details







6.4 Successfully configures the auto scaling group.



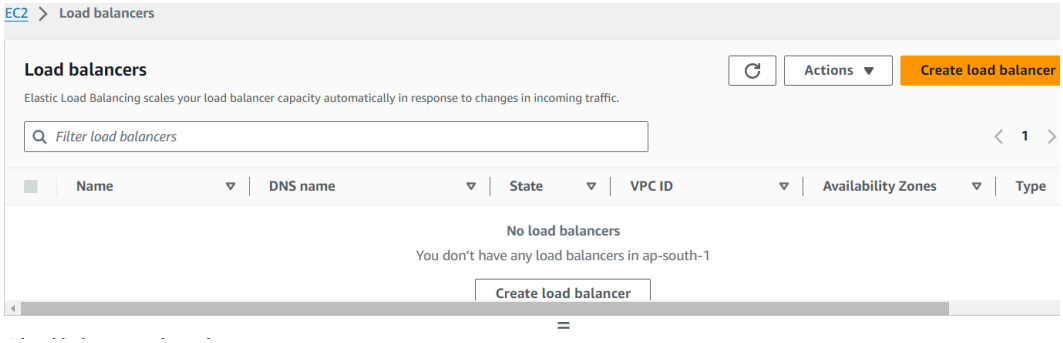
7. Load Balancer Configuration

Load Balancer Configuration:

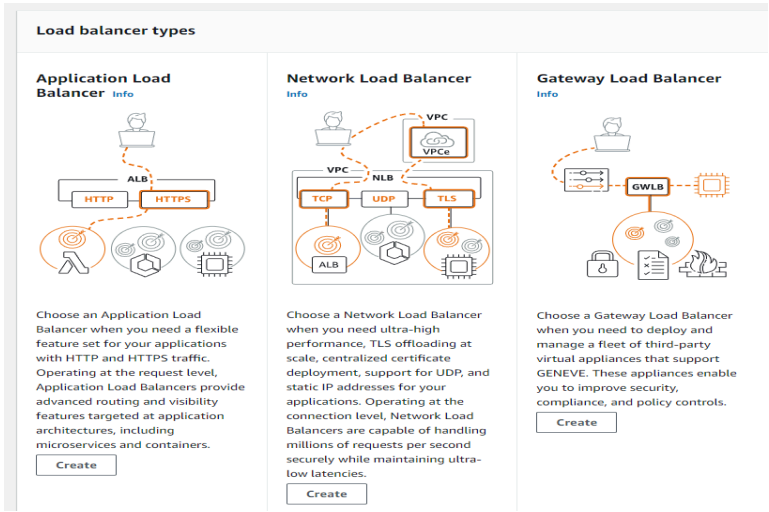
- Click the **Create Load Balancer** button and Select **Application Load Balancer** and assign the name, configure HTTP and HTTPS in security group under inbound rules
- Create a Target group to register the instances and provision the health checks.
- Go back to the Load balancer page and add the listeners and review the configuration and click **Create Load Balancer**.

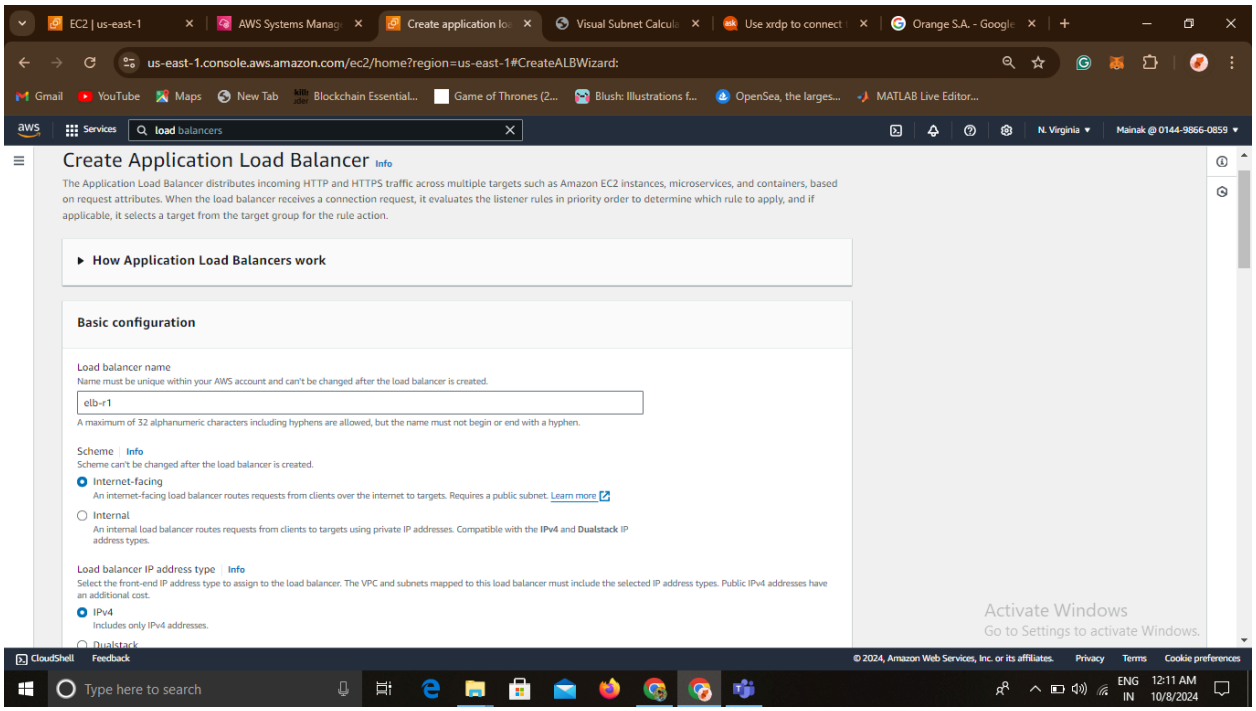
Step 7: Launch ELB to distribute Load

7.1 In the EC2 left pane scroll down to find **Load Balancer** click on it and create load balancer.

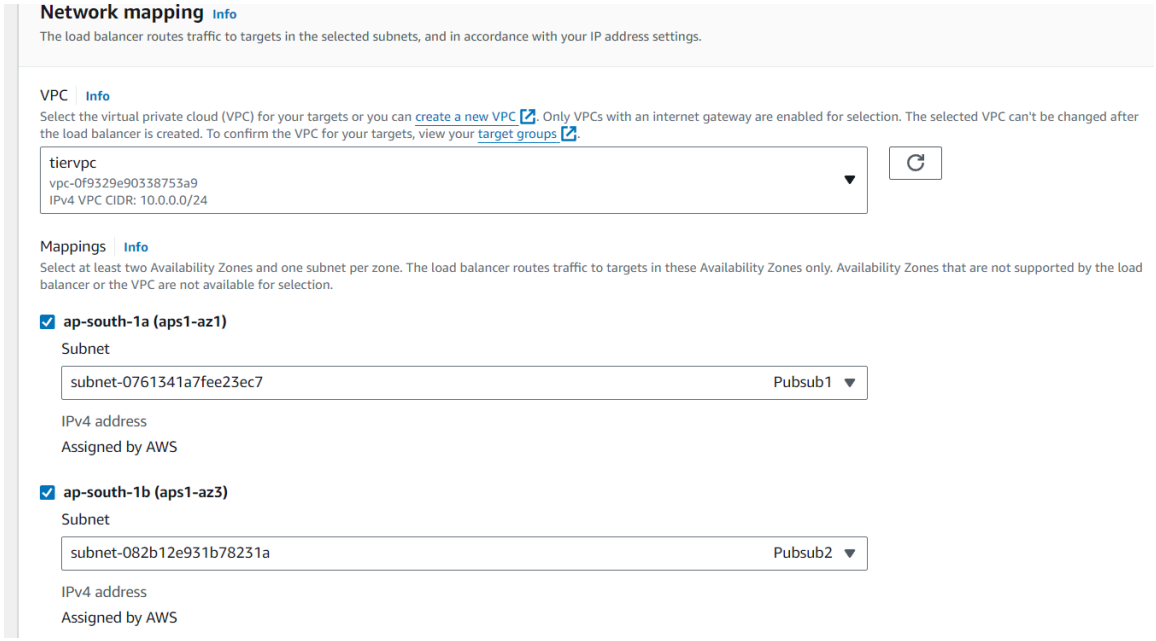


7.2 So here, we will choose **Application Load Balancer** to request HTTP traffic.

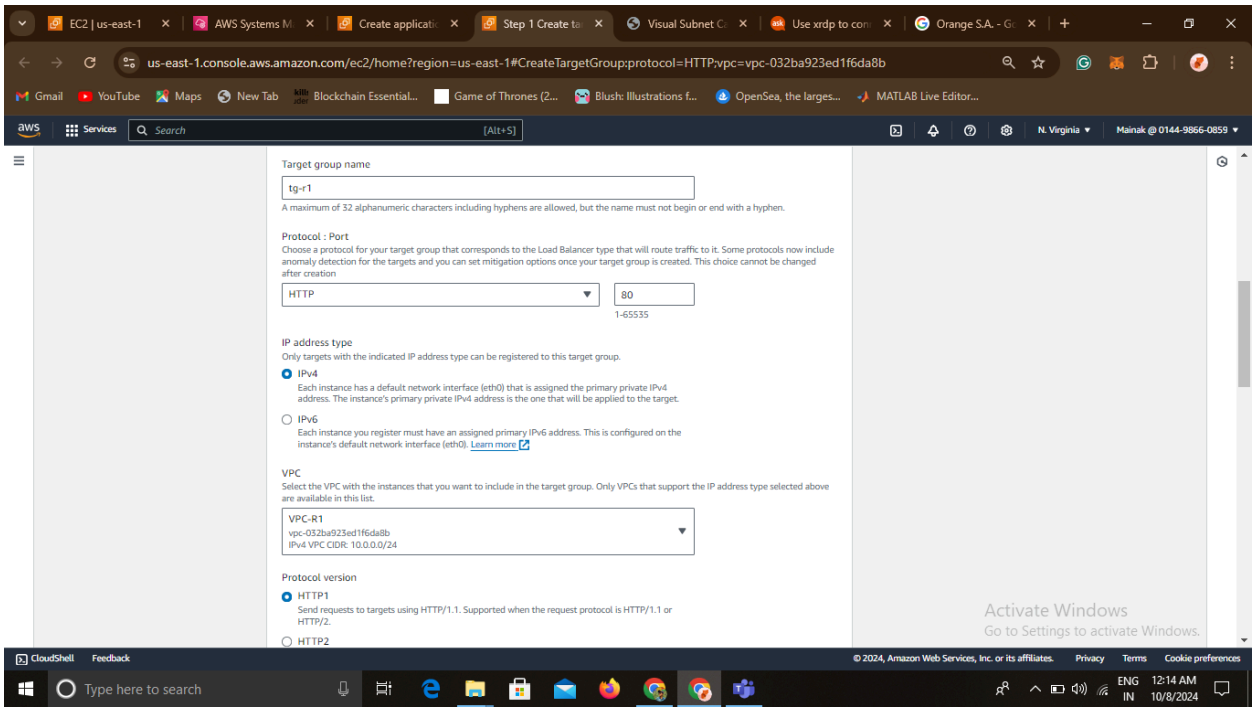




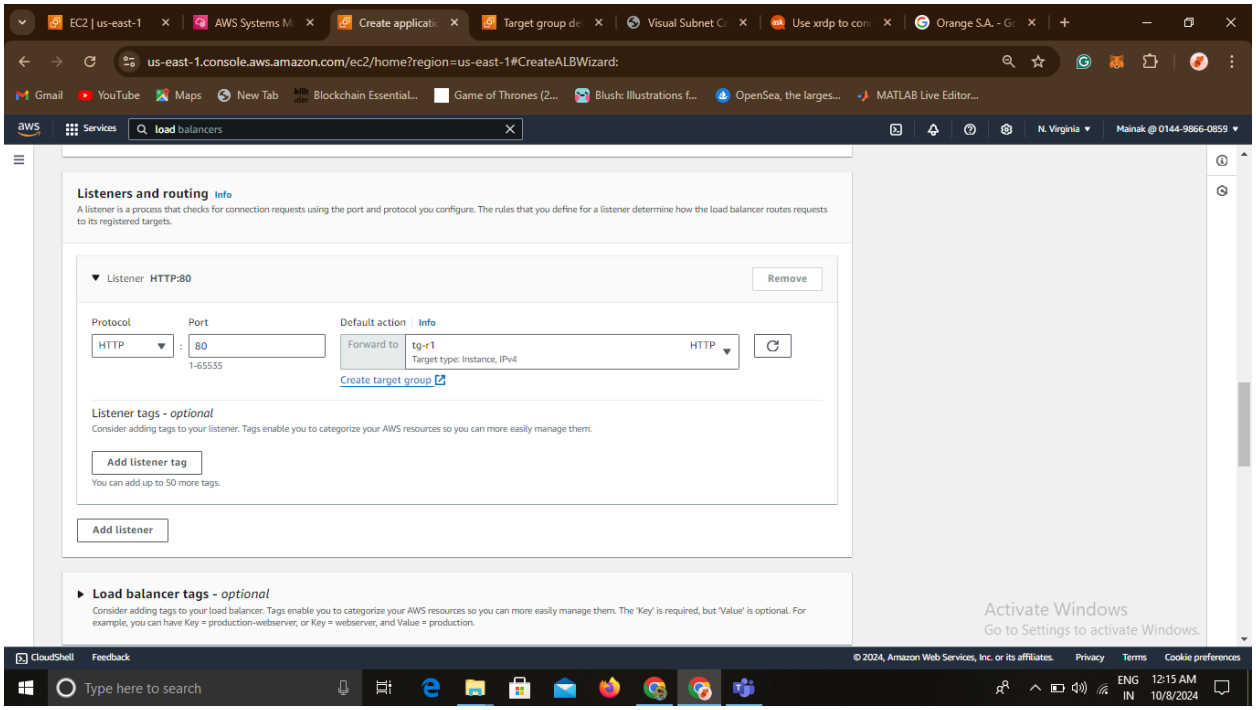
7.3 Add the VPC and the mappings for Availability zones with the existing security group

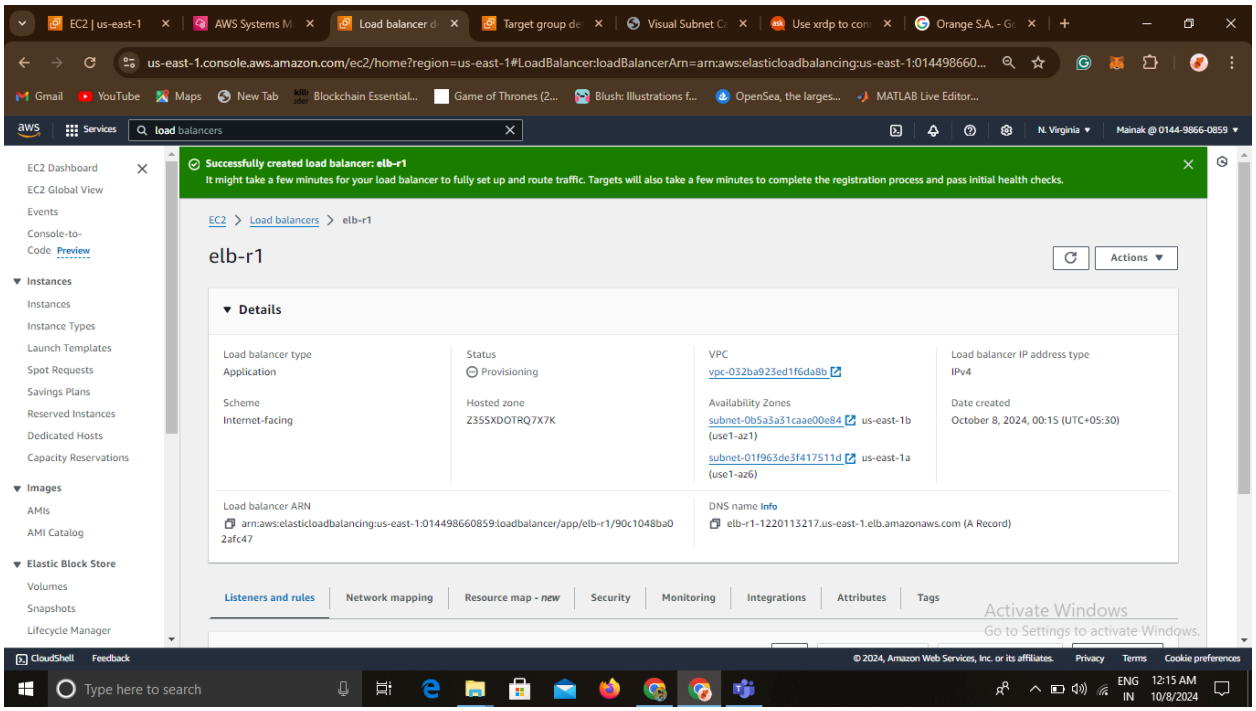


7.4 Create a **Target group** with register targets, Click **Next** and then register the targets by **Include as pending below**.

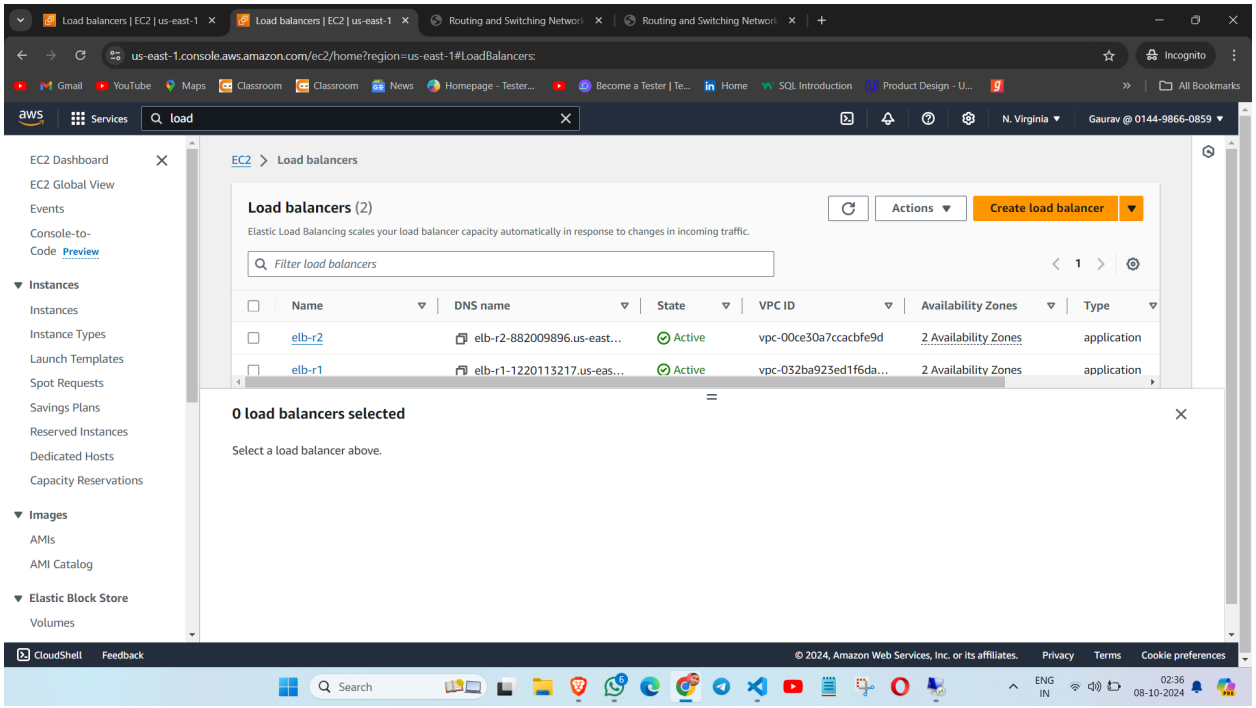


7.5 Now associate the build **Target group** in Application load balancer and click **Create Load balancer.**



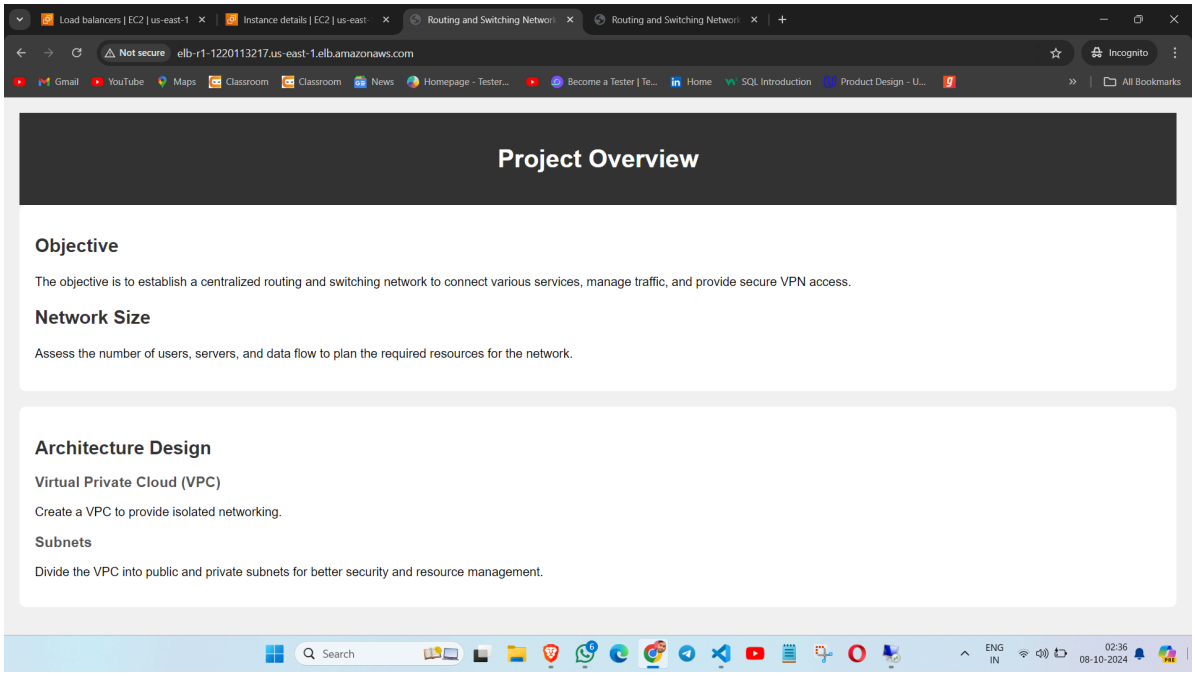


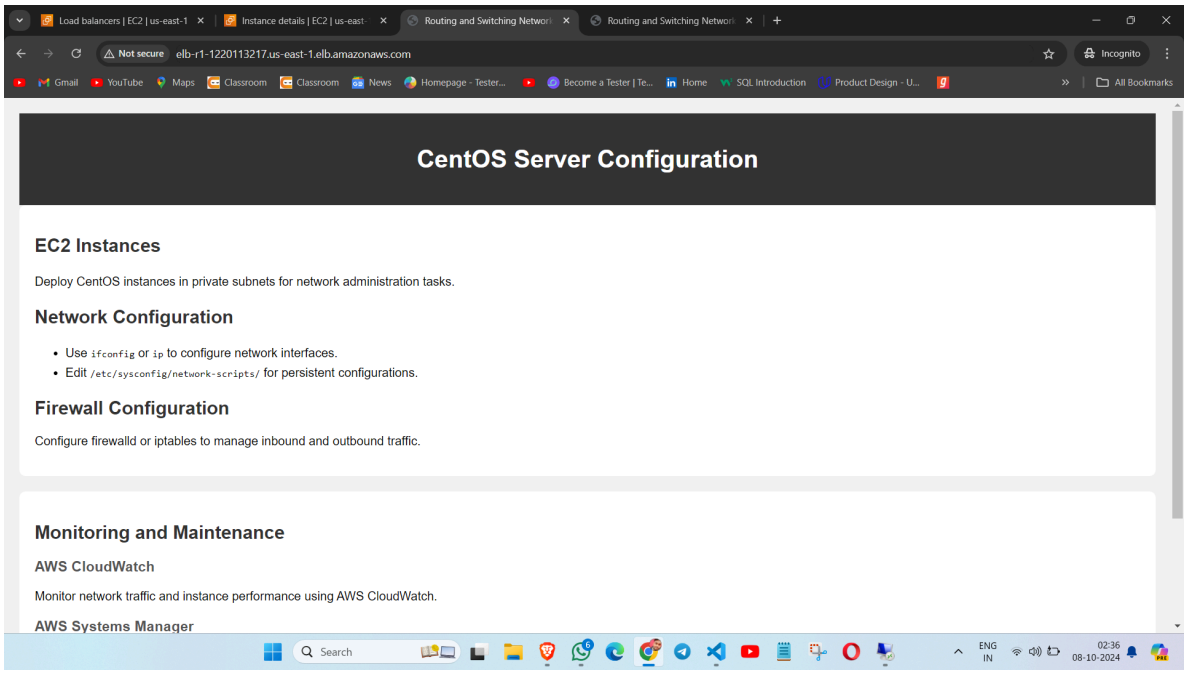
7.6 Similarly, configure one more load balancer for other 2 EC2 instances.



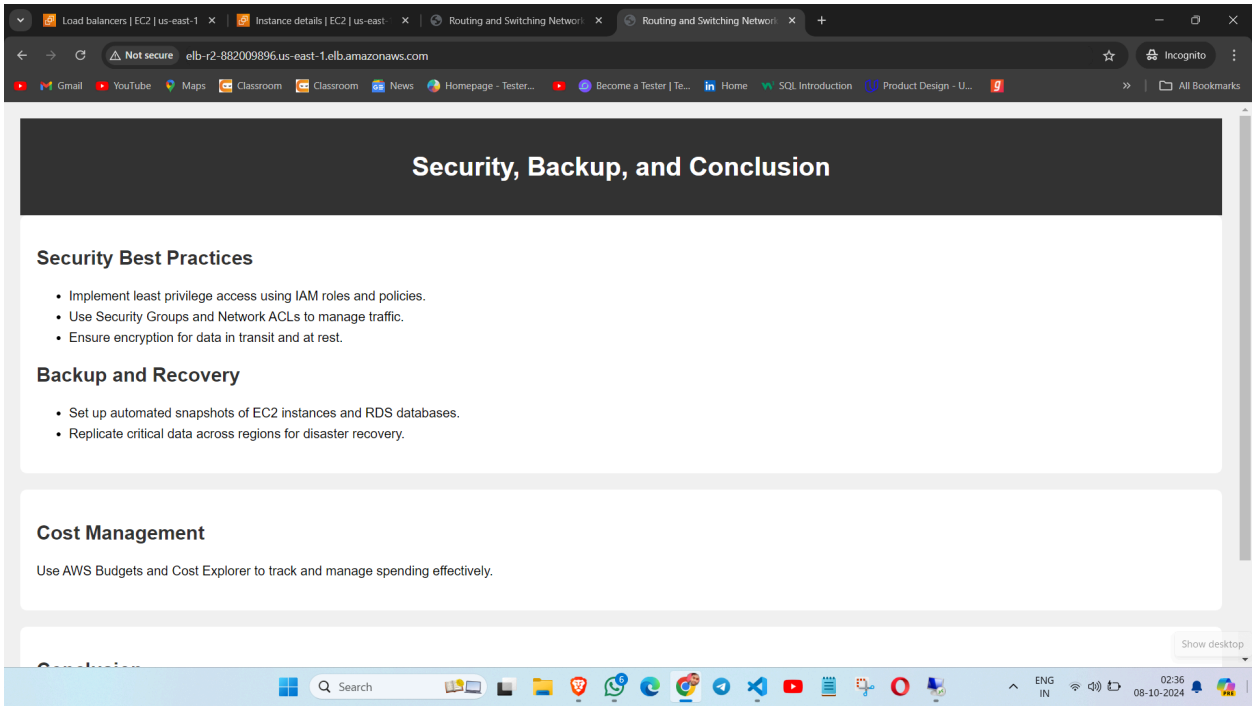
7.7 Now, copy the DNS name and paste it in a new tab to check the distribution of load.

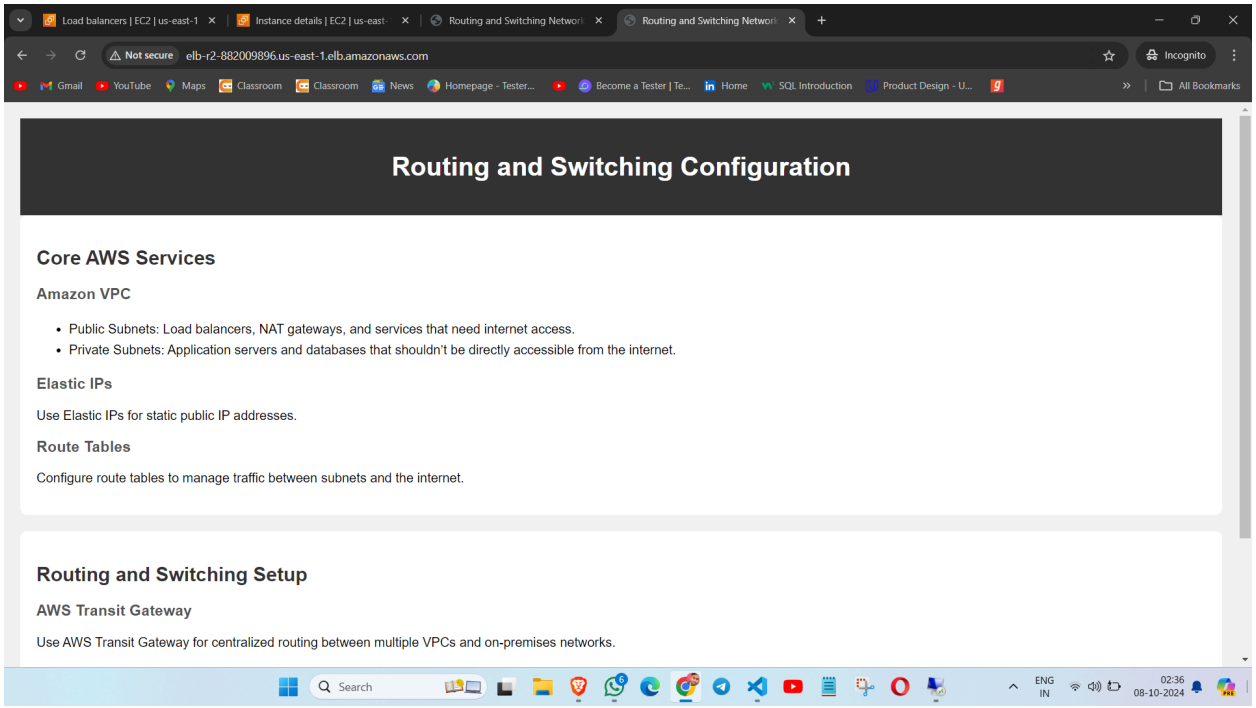
ELB-1


Load balancers | EC2 | us-east-1
Instance details | EC2 | us-east-
Routing and Switching Network
Routing and Switching Network
Not secure
elb-r1-1220113217.us-east-1.elb.amazonaws.com
Incognito
Gmail
YouTube
Maps
Classroom
Classroom
News
Homepage - Tester...
Become a Tester | Te...
Home
SQL Introduction
Product Design - U...
All Bookmarks
Project Overview
Objective
The objective is to establish a centralized routing and switching network to connect various services, manage traffic, and provide secure VPN access.
Network Size
Assess the number of users, servers, and data flow to plan the required resources for the network.
Architecture Design
Virtual Private Cloud (VPC)
Create a VPC to provide isolated networking.
Subnets
Divide the VPC into public and private subnets for better security and resource management.
Search
ENG
IN
02:36
08-10-2024


Load balancers | EC2 | us-east-1
Instance details | EC2 | us-east-
Routing and Switching Network
Routing and Switching Network
Not secure
elb-r1-1220113217.us-east-1.elb.amazonaws.com
Incognito
Gmail
YouTube
Maps
Classroom
Classroom
News
Homepage - Tester...
Become a Tester | Te...
Home
SQL Introduction
Product Design - U...
All Bookmarks
CentOS Server Configuration
EC2 Instances
Deploy CentOS instances in private subnets for network administration tasks.
Network Configuration
Use ifconfig or ip to configure network interfaces.
Edit /etc/sysconfig/network-scripts/ for persistent configurations.
Firewall Configuration
Configure firewalld or iptables to manage inbound and outbound traffic.
Monitoring and Maintenance
AWS CloudWatch
Monitor network traffic and instance performance using AWS CloudWatch.
AWS Systems Manager
Search
ENG
IN
02:36
08-10-2024

ELB-2


Load balancers | EC2 | us-east-1
Instance details | EC2 | us-east-
Routing and Switching Networ
Routing and Switching Networ
Not secure
elb-r2-882009896.us-east-1.elb.amazonaws.com
Incognito
Gmail
YouTube
Maps
Classroom
Classroom
News
Homepage - Tester...
Become a Tester | Te...
Home
SQL Introduction
Product Design - U...
All Bookmarks
Security, Backup, and Conclusion
Security Best Practices
Implement least privilege access using IAM roles and policies.
Use Security Groups and Network ACLs to manage traffic.
Ensure encryption for data in transit and at rest.
Backup and Recovery
Set up automated snapshots of EC2 instances and RDS databases.
Replicate critical data across regions for disaster recovery.
Cost Management
Use AWS Budgets and Cost Explorer to track and manage spending effectively.
Show desktop
Search
ENG
IN
02:36
08-10-2024


Load balancers | EC2 | us-east-1
Instance details | EC2 | us-east-
Routing and Switching Networ
Routing and Switching Networ
Not secure
elb-r2-882009896.us-east-1.elb.amazonaws.com
Incognito
Gmail
YouTube
Maps
Classroom
Classroom
News
Homepage - Tester...
Become a Tester | Te...
Home
SQL Introduction
Product Design - U...
All Bookmarks
Routing and Switching Configuration
Core AWS Services
Amazon VPC
Public Subnets: Load balancers, NAT gateways, and services that need internet access.
Private Subnets: Application servers and databases that shouldn't be directly accessible from the internet.
Elastic IPs
Use Elastic IPs for static public IP addresses.
Route Tables
Configure route tables to manage traffic between subnets and the internet.
Routing and Switching Setup
AWS Transit Gateway
Use AWS Transit Gateway for centralized routing between multiple VPCs and on-premises networks.
Search
ENG
IN
02:36
08-10-2024

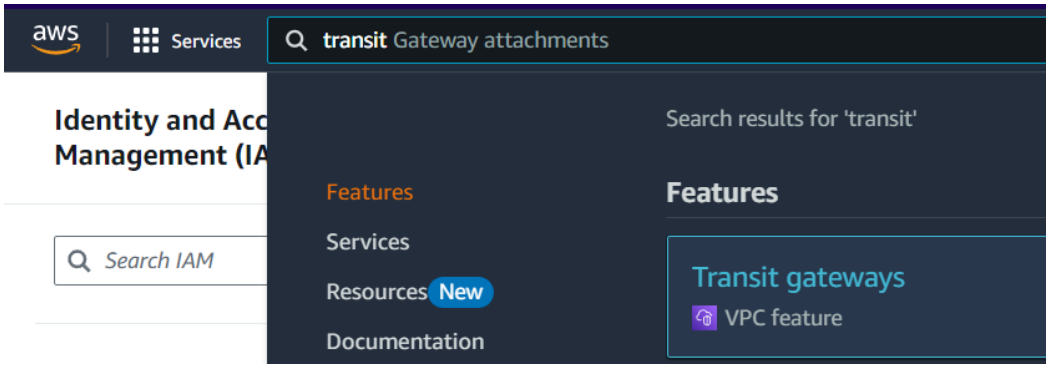
8. Transit Gateway Configuration

Transit Gateway Configuration:

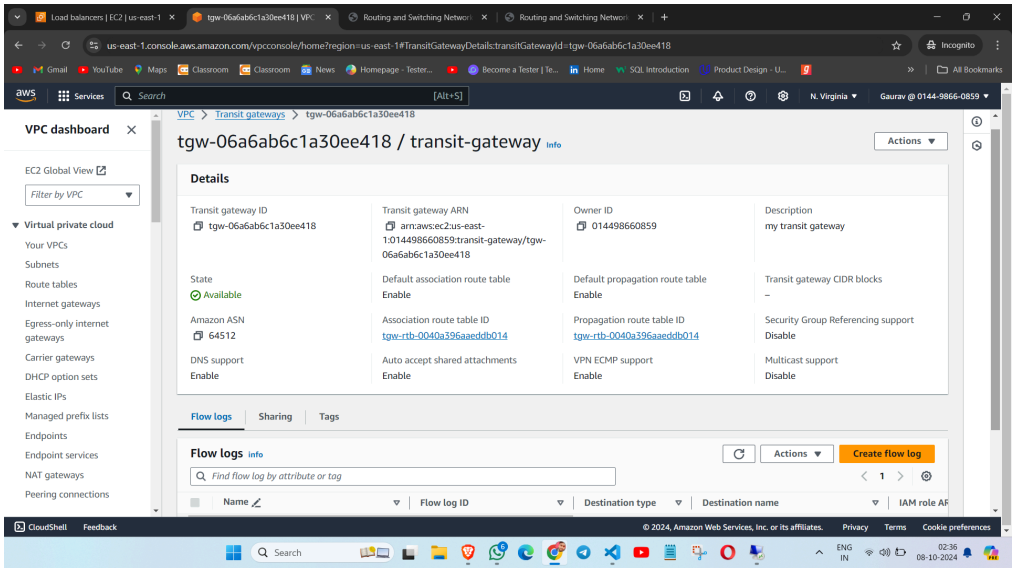
- In the VPC page, click on Transit Gateway to assign a name.
- Enter the ASN for Transit Gateway, then create transit gateway attachments, attach the VPCs that we created.
- Create the attachment and configure the security group for it.

Step 8: Launch Transit Gateway in Console

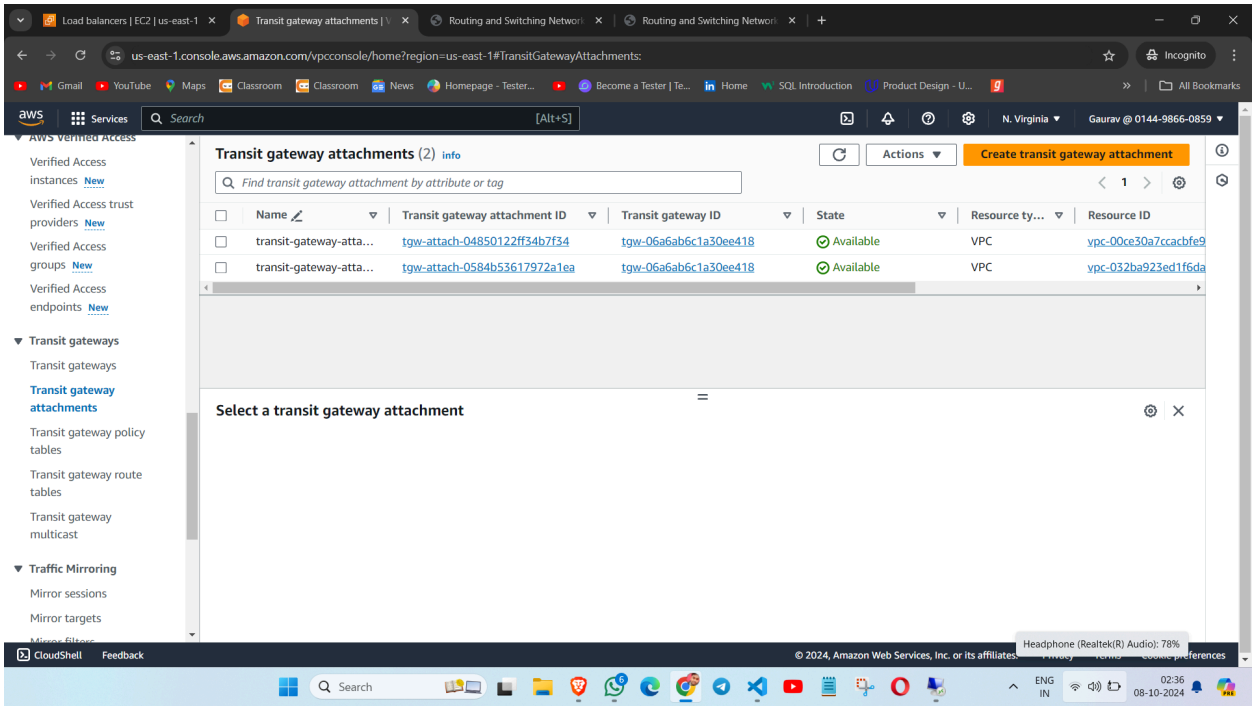
8.1 In Dashboard, search for Transit Gateway service, click **VPC** to open it.



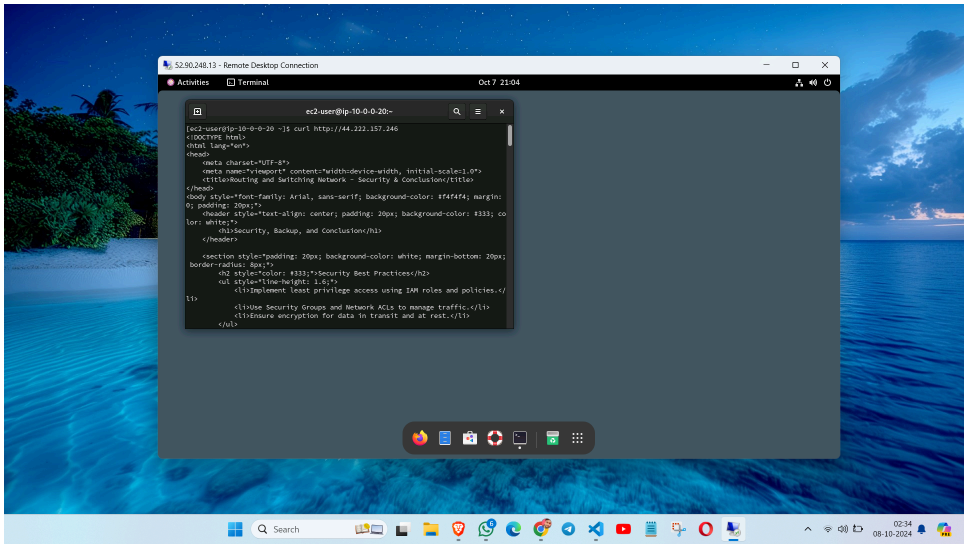
8.2 Create a transit gateway with default ASN 64512 and attach the VPC

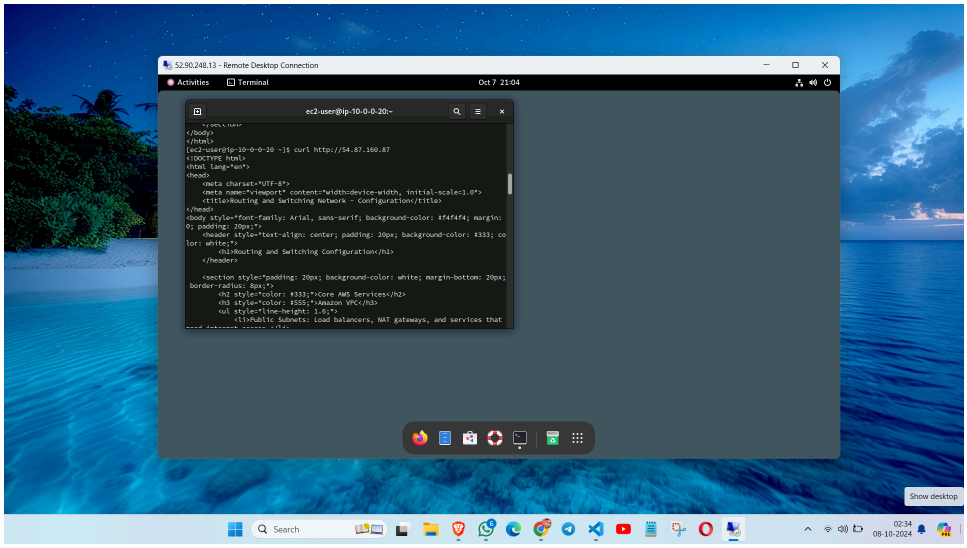


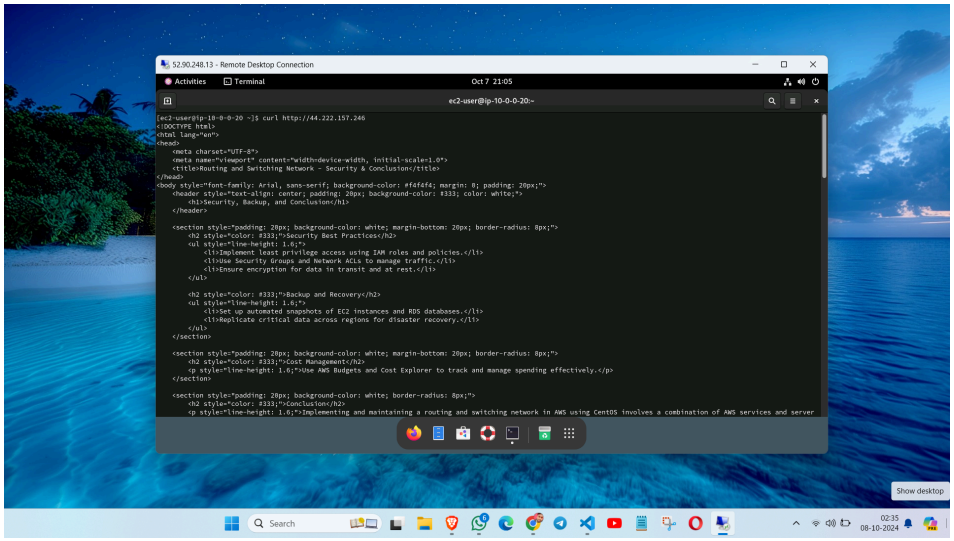
8.3 Configure the attachments for the 2 VPCs

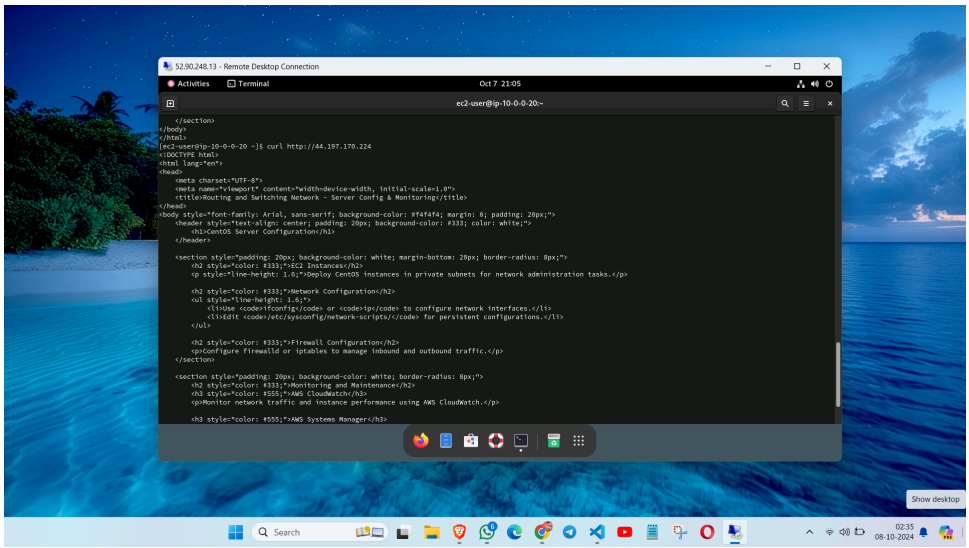


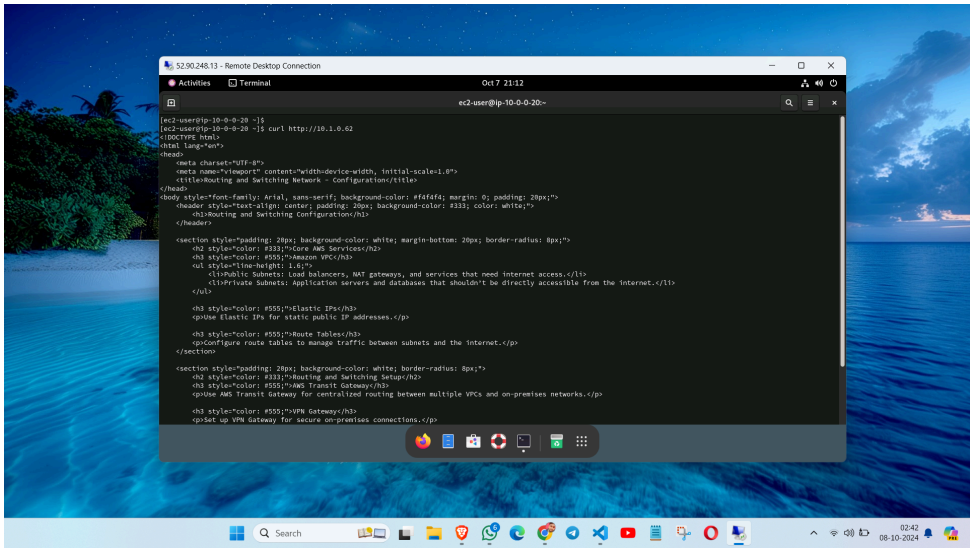
8.4 To test the connectivity open the EC2 instance ping the ip addresses of different VPC.




52.90.248.13 - Remote Desktop Connection
Activities
Terminal
Oct 7 21:04
ec2-user@ip-10-0-0-20:~
[ec2-user@ip-10-0-0-20 ~]$ curl http://54.87.160.87
Routing and Switching Configuration
Core AWS Services
Amazon VPC
Public Subnets: Load balancers, NAT gateways, and services that
Show desktop
Search
02:34
08-10-2024


52.90.248.13 - Remote Desktop Connection
Activities
Terminal
Oct 7 21:05
ec2-user@ip-10-0-0-20:~
[ec2-user@ip-10-0-0-20 ~]$ curl http://44.222.157.246
Routing and Switching Network - Security & Conclusion
Security, Backup, and Conclusion
Security Best Practices
Implement least privilege access using IAM roles and policies.
Use Security Groups and Network ACLs to manage traffic.
Ensure encryption for data in transit and at rest.
Backup and Recovery
Set up automated snapshots of EC2 instances and RDS databases.
Replicate critical data across regions for disaster recovery.
Cost Management
Use AWS Budgets and Cost Explorer to track and manage spending effectively.
Conclusion
Implementing and maintaining a routing and switching network in AWS using CentOS involves a combination of AWS services and server
Show desktop
Search
02:35
08-10-2024


52.90.248.13 - Remote Desktop Connection
Activities
Terminal
Oct 7 21:05
ec2-user@ip-10-0-0-20:~
[ec2-user@ip-10-0-0-20 ~]$ curl http://44.197.170.224
Routing and Switching Network - Server Config & Monitoring
CentOS Server Configuration
EC2 Instances
Deploy CentOS instances in private subnets for network administration tasks.
Network Configuration
Use ifconfig or ip to configure network interfaces.
Edit /etc/sysconfig/network-scripts/ for persistent configurations.
Firewall Configuration
Configure firewalld or iptables to manage inbound and outbound traffic.
Monitoring and Maintenance
AWS CloudWatch
Monitor network traffic and instance performance using AWS CloudWatch.
AWS Systems Manager
Show desktop
Search
02:35
08-10-2024


52.90.248.13 - Remote Desktop Connection
Activities
Terminal
Oct 7 21:12
ec2-user@ip-10-0-0-20:~
[ec2-user@ip-10-0-0-20 ~]$
[ec2-user@ip-10-0-0-20 ~]$ curl http://10.1.0.62
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>Routing and Switching Network - Configuration</title>
</head>
<body style="font-family: Arial, sans-serif; background-color: #f4f4f4; margin: 0; padding: 20px;">
<header style="text-align: center; padding: 20px; background-color: #333; color: white;">
<h1>Routing and Switching Configuration</h1>
</header>
<section style="padding: 20px; background-color: white; margin-bottom: 20px; border-radius: 8px;">
<h2 style="color: #333;">Core AWS Services</h2>
<h3 style="color: #555;">Amazon VPC</h3>
<ul style="line-height: 1.6;">
Public Subnets: Load balancers, NAT gateways, and services that need internet access.
Private Subnets: Application servers and databases that shouldn't be directly accessible from the internet.

<h3 style="color: #555;">Elastic IPs</h3>
Use Elastic IPs for static public IP addresses.
<h3 style="color: #555;">Route Tables</h3>
Configure route tables to manage traffic between subnets and the internet.
</section>
<section style="padding: 20px; background-color: white; border-radius: 8px;">
<h2 style="color: #333;">Routing and Switching Setup</h2>
<h3 style="color: #555;">AWS Transit Gateway</h3>
Use AWS Transit Gateway for centralized routing between multiple VPCs and on-premises networks.
<h3 style="color: #555;">VPN Gateway</h3>
Set up VPN Gateway for secure on-premises connections.
Search
02:42
08-10-2024

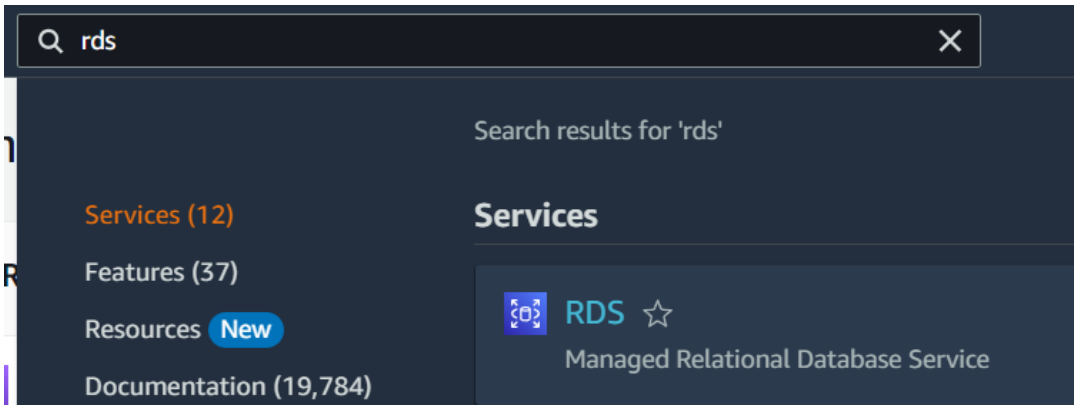
9. RDS Configuration

RDS Configuration:

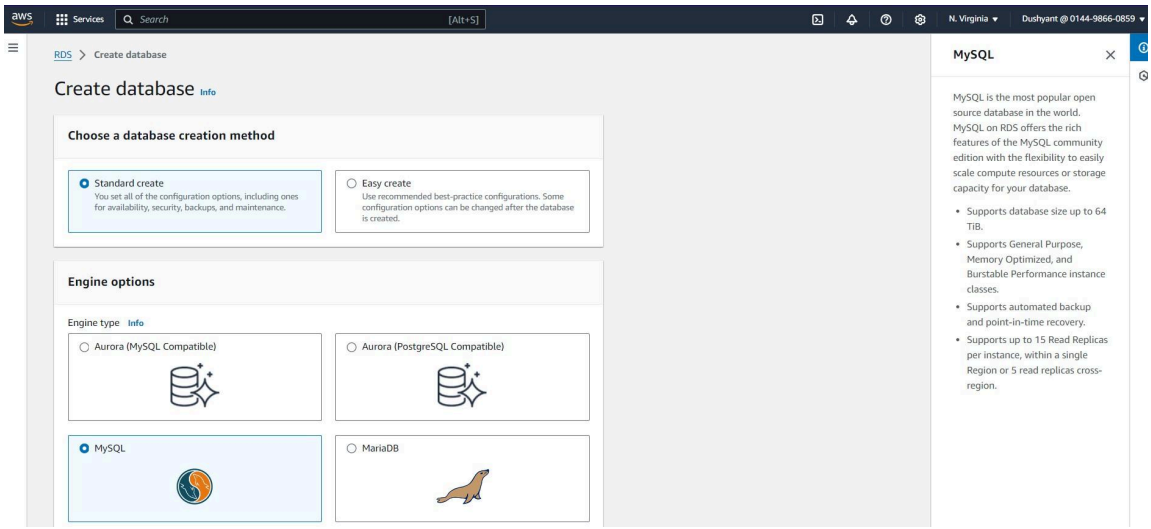
- Click on Databases and choose the Standard creation method.
- Select the MySQL database engine and specify the DB details.
- Add the VPC and custom as well as default security groups and configure the backup snapshots.
- Also configure the Read replica of the RDS in different region

Step 9: Launch RDS to build the database

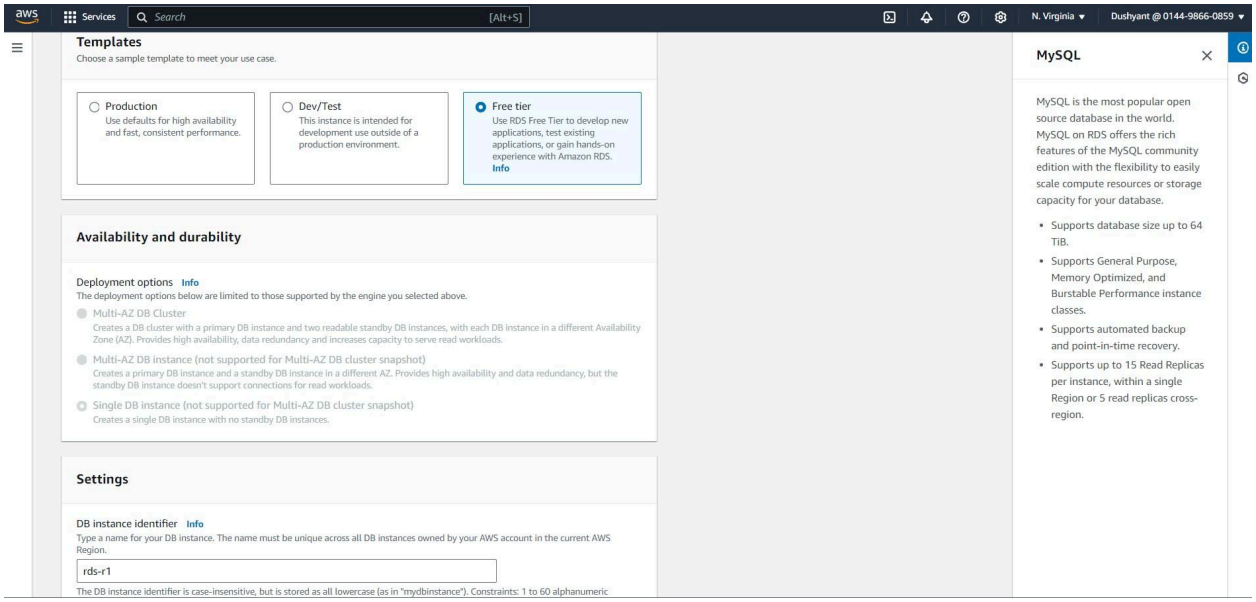
9.1 In Dashboard, search for RDS service, click **RDS** to open it.



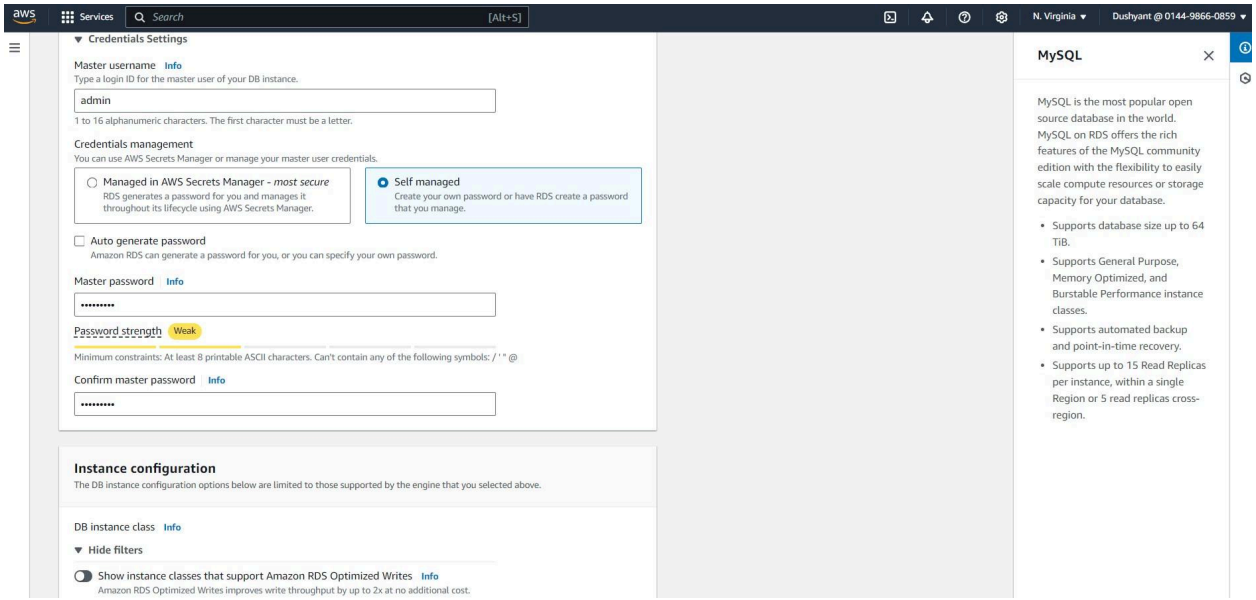
9.2 Keep the database creation **Standard create** and select engine as **MySQL**.



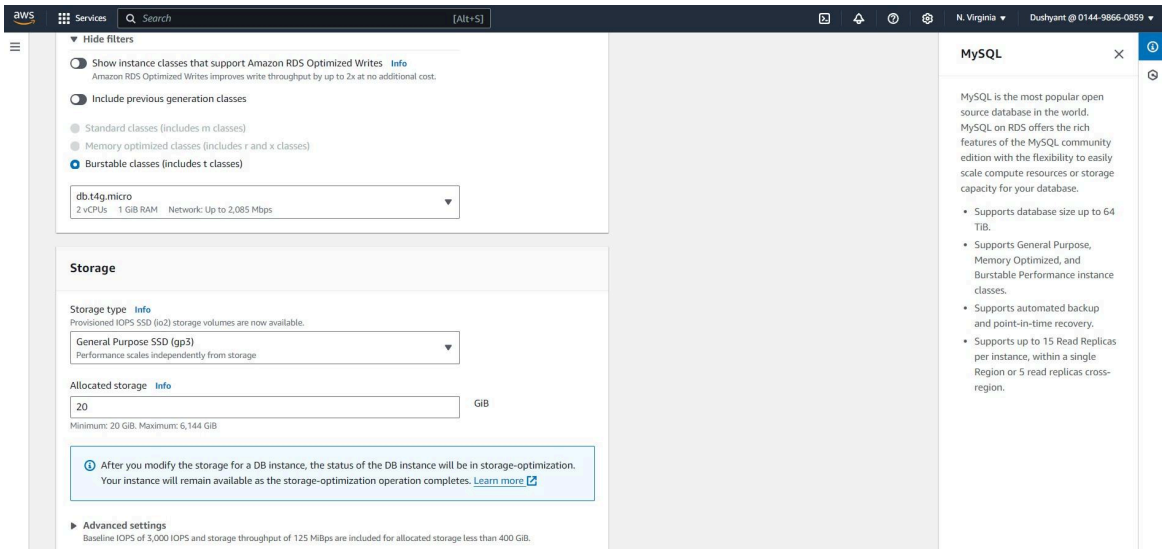
9.3 Now, under the templates select **Free tier**, with the db instance as **rds-r1**.



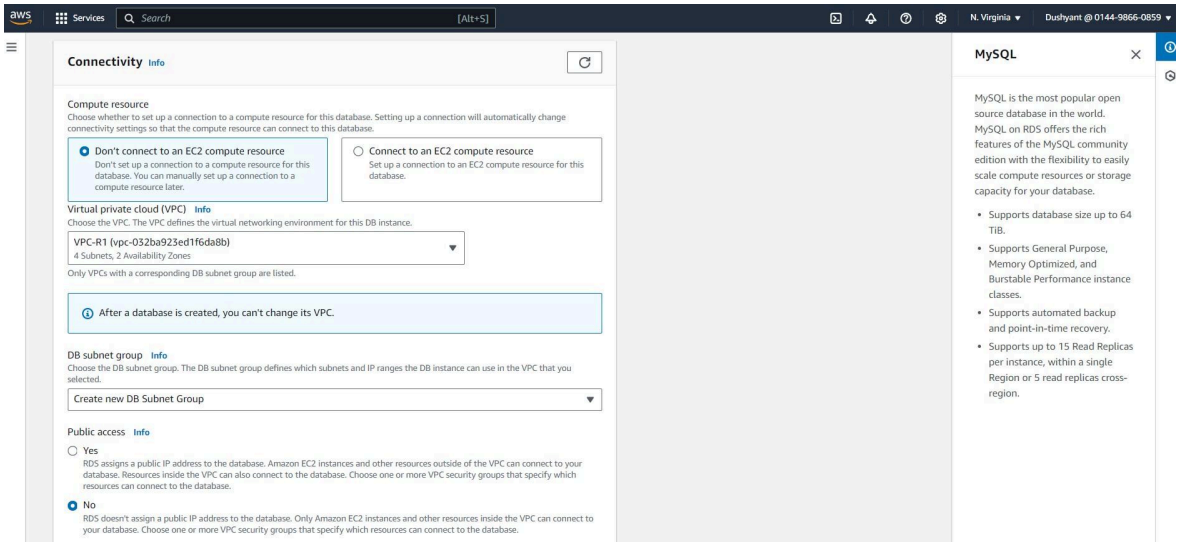
9.4 Add the credentials for database creation with password

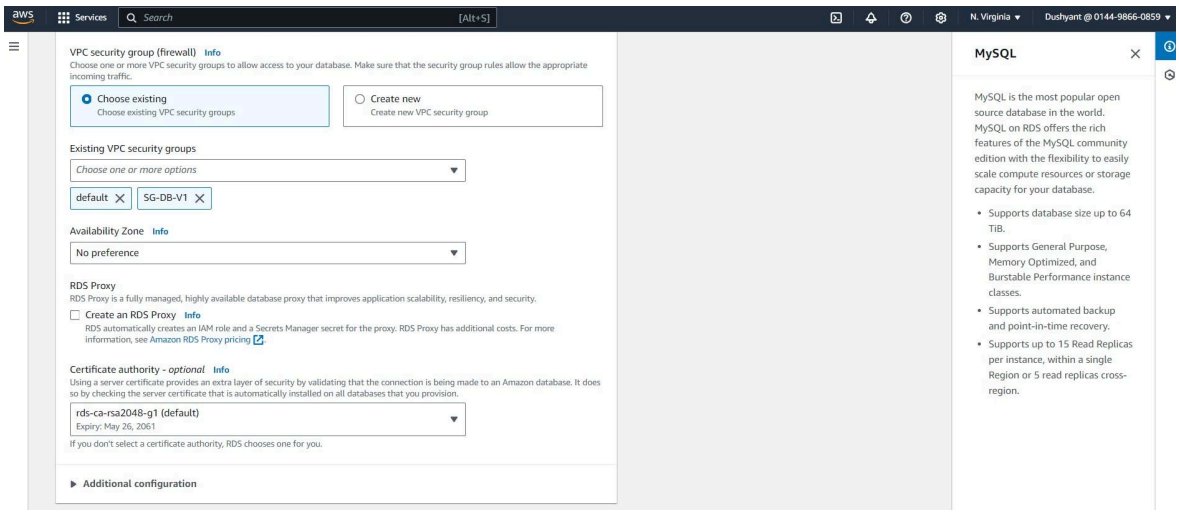


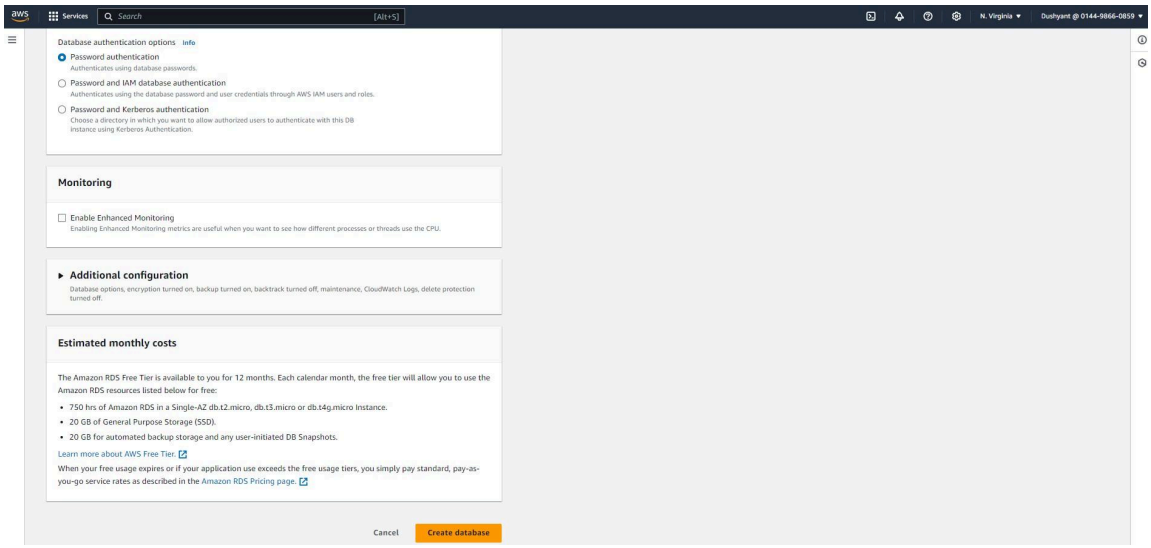
9.5 Make the instance configuration to default **Bustable classes**.



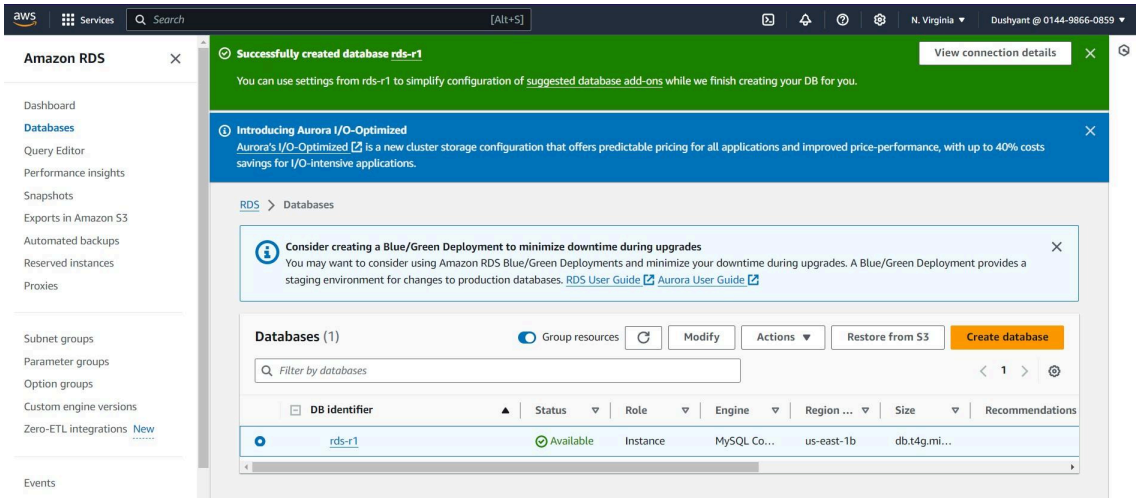
9.6 Similarly, attach the VPC made before here as well and rest leave it default and click **create a database**.



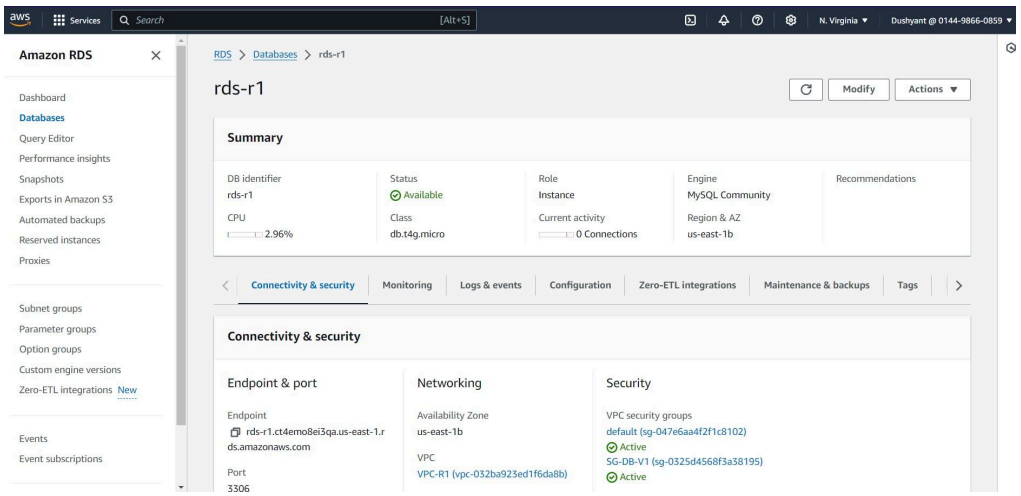




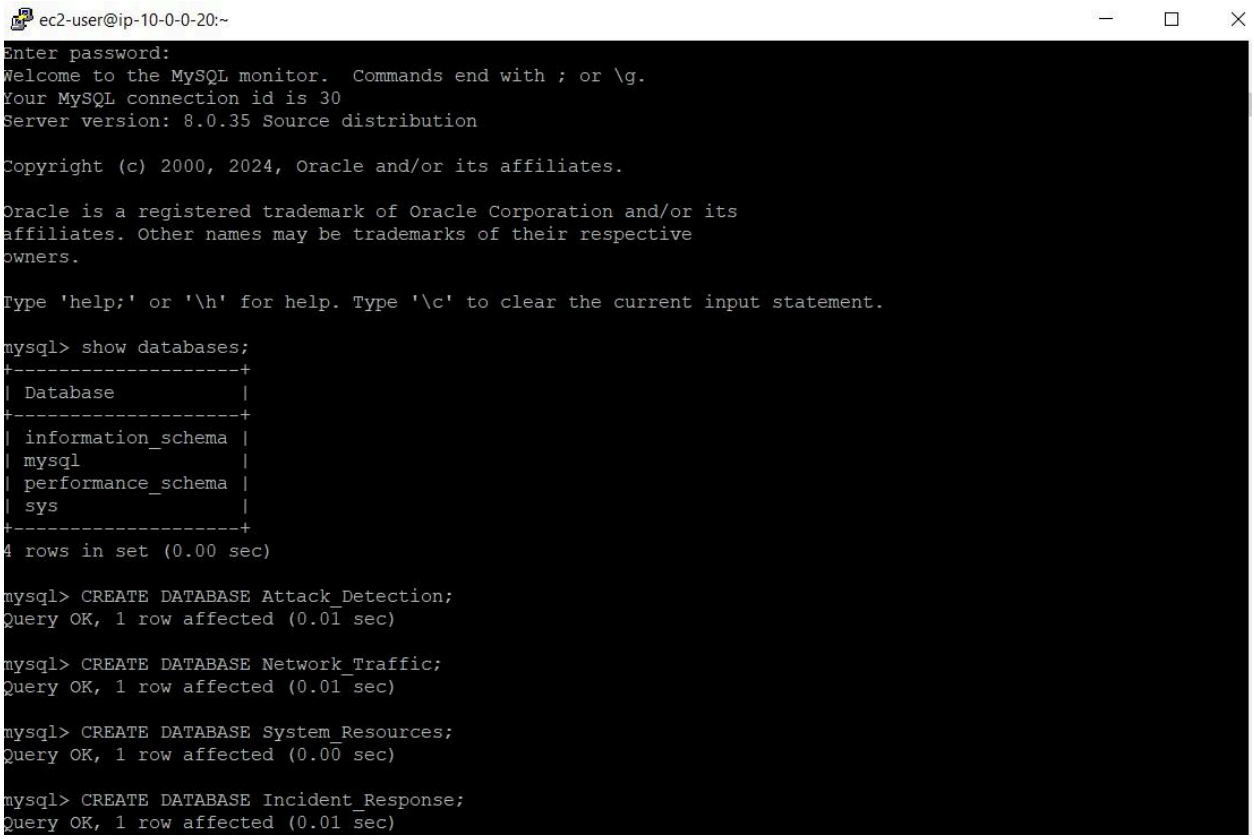
9.7 Successfully created the database.



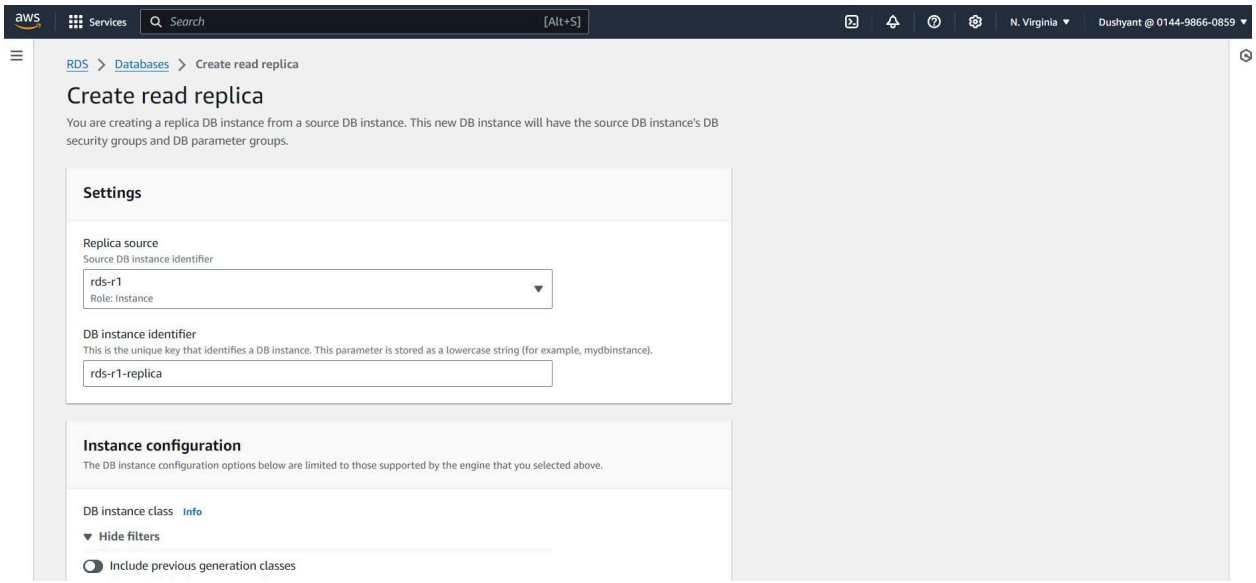
9.8 Wait for some time then the endpoint will also get updated.

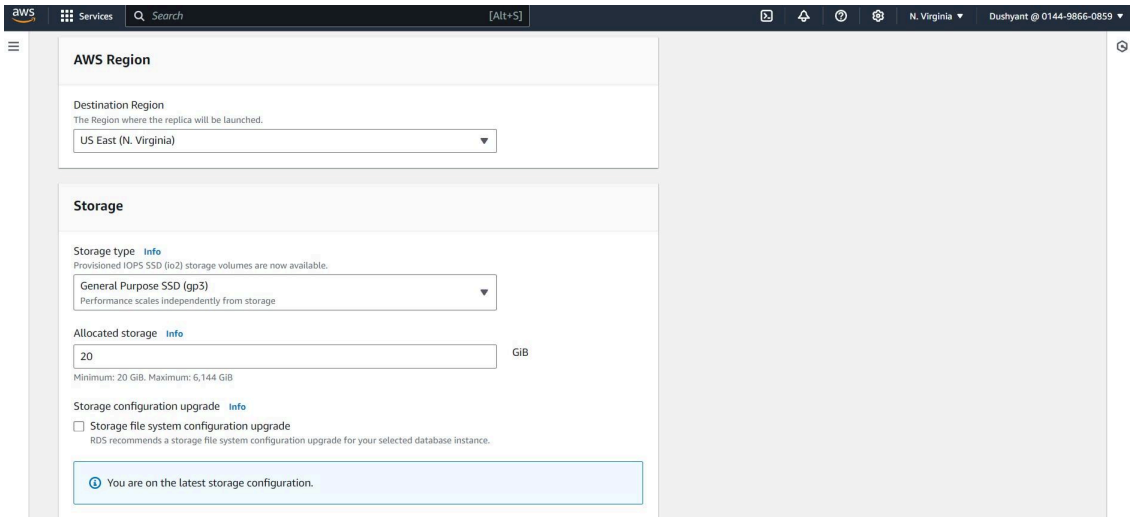


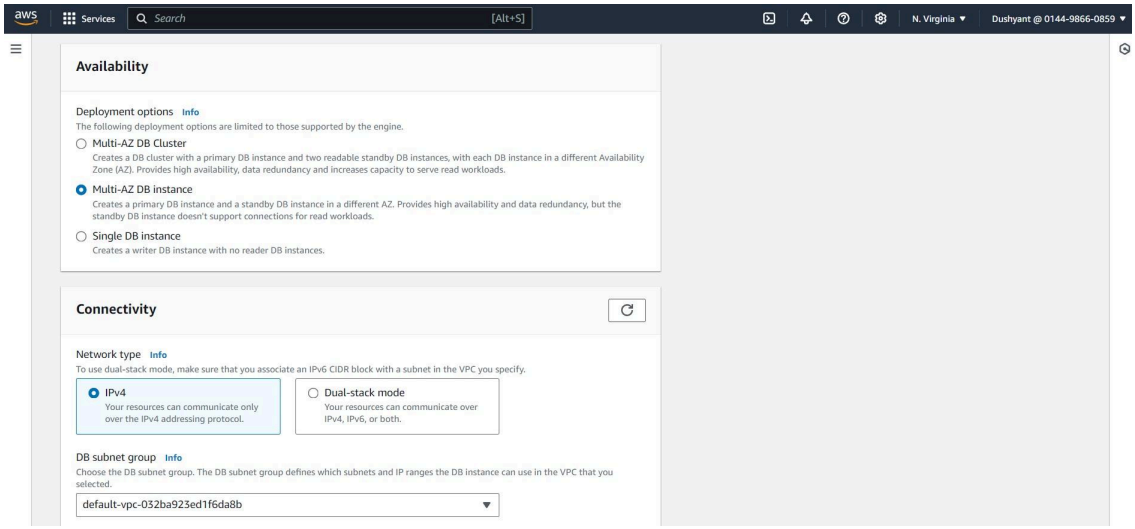
9.9 Now, open EC2 instance and connect it and type the commands to connect "**mysql -h (endpoint of database) -P 3306 -u admin -p**"



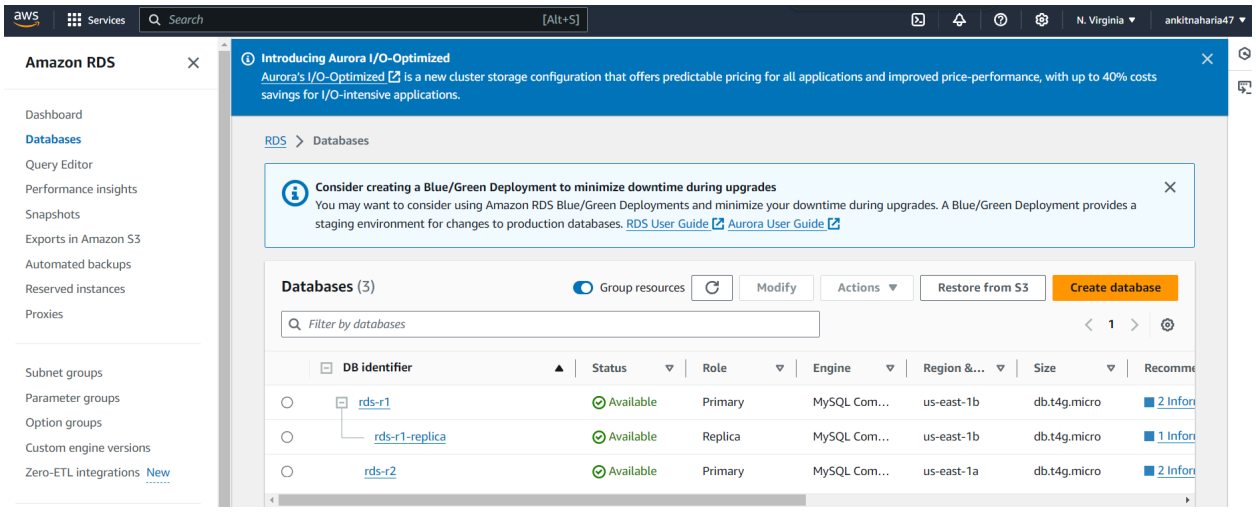
9.10 Now, create a **Replica DB instance** for processing the primary DB data into it.

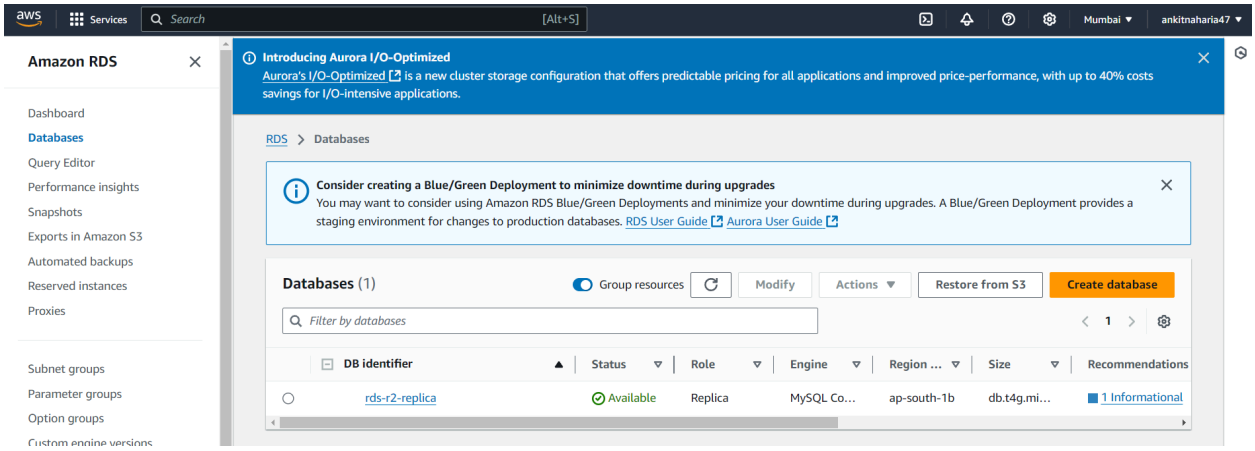




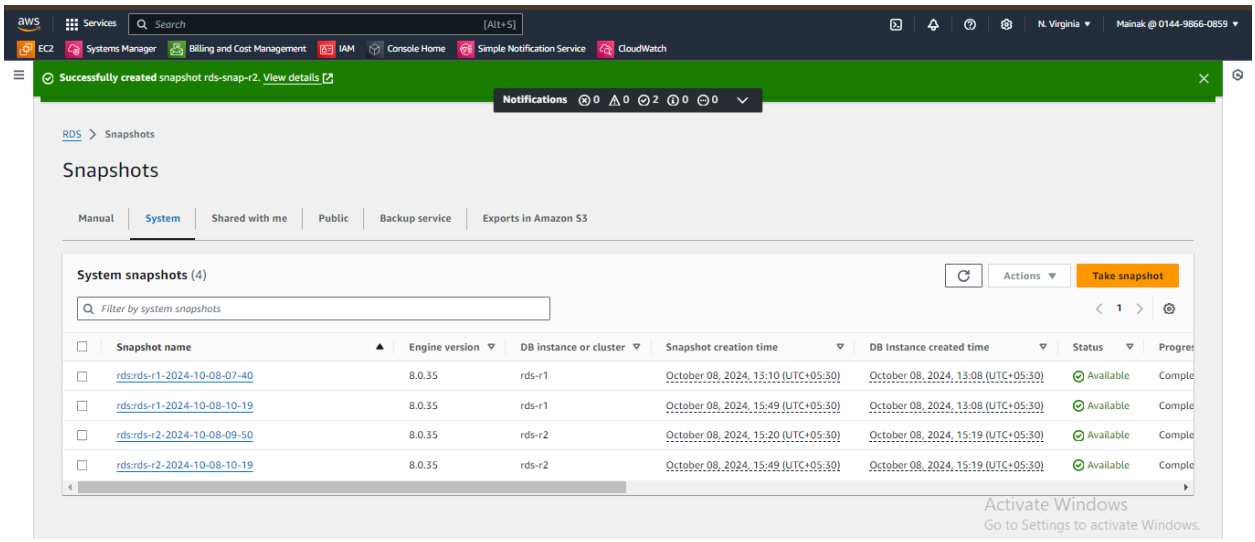


9.11 Successfully created the replica database '**rds-r1-replica**'. Similarly create one more replica.





9.12 To keep the backup of the database also created snapshots of the RDS.



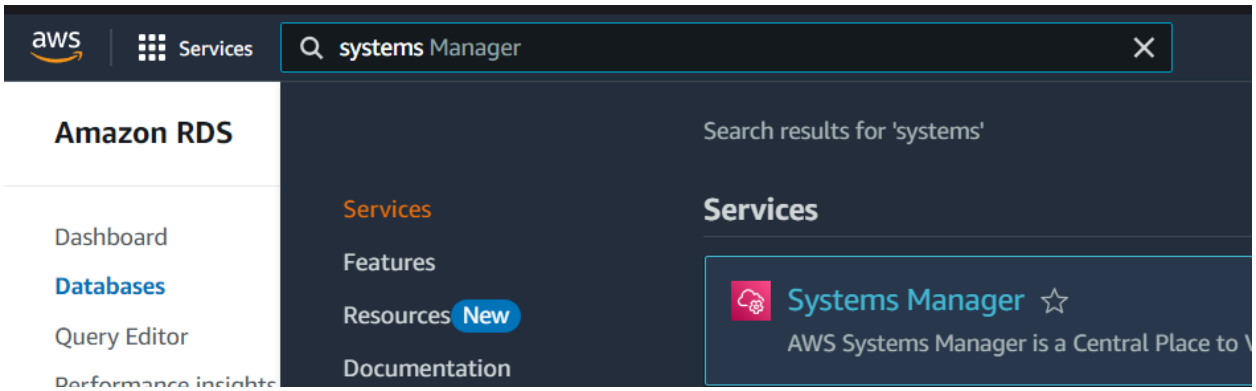
10. Systems Manager Configuration

Systems Manager Configuration:

- Go to the EC2 and connect via SSM Agent and check the status of the instance.
- Then go to Systems Manager and streamline the fleet manager in Node management to understand the file system hierarchy used in CentOS configuration

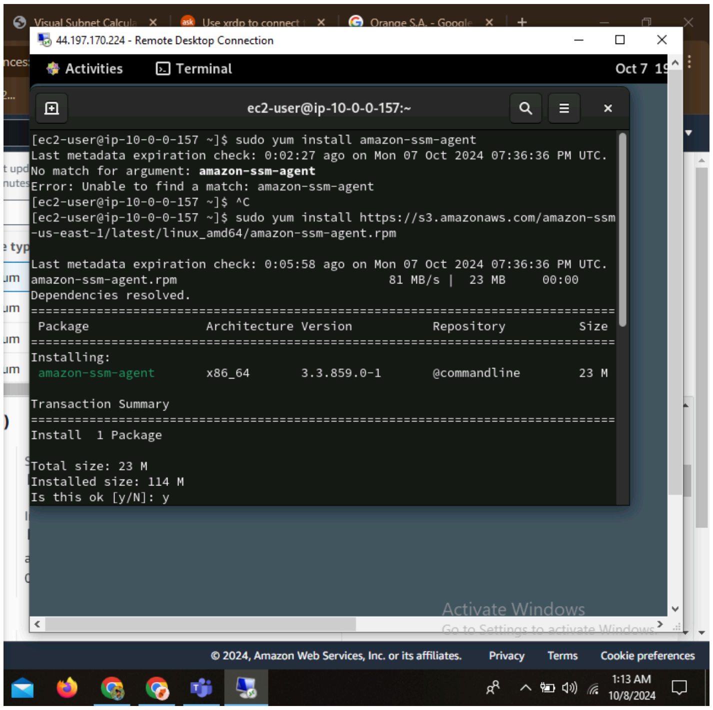
Step 10: Launch Fleet Manager under Node Management in Console

10.1 In Dashboard, search for Systems Manager service, click **Systems Manager** to open it.



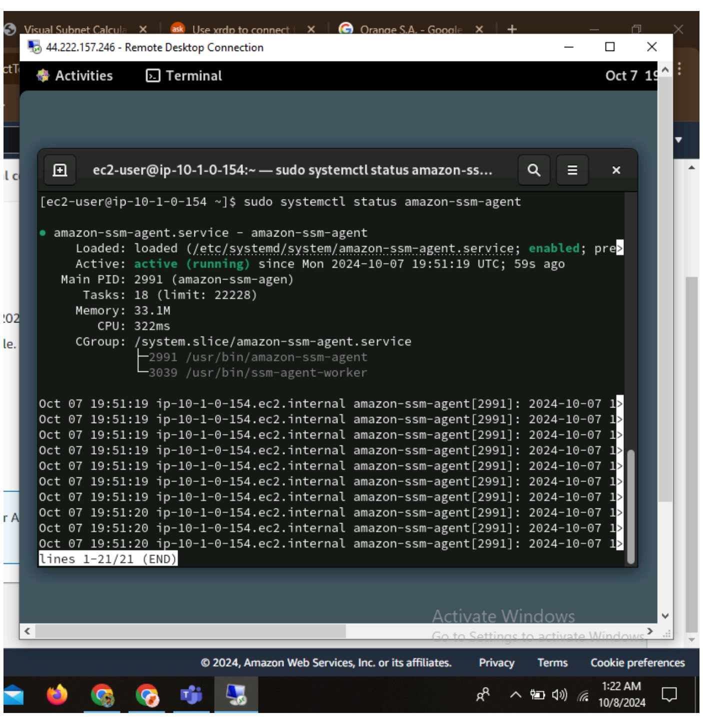
10.2 Access the file structure hierarchy to do that SSM Agent has to be configured in EC2. Type in the command:

```
sudo yum install amazon-ssm-agent
```



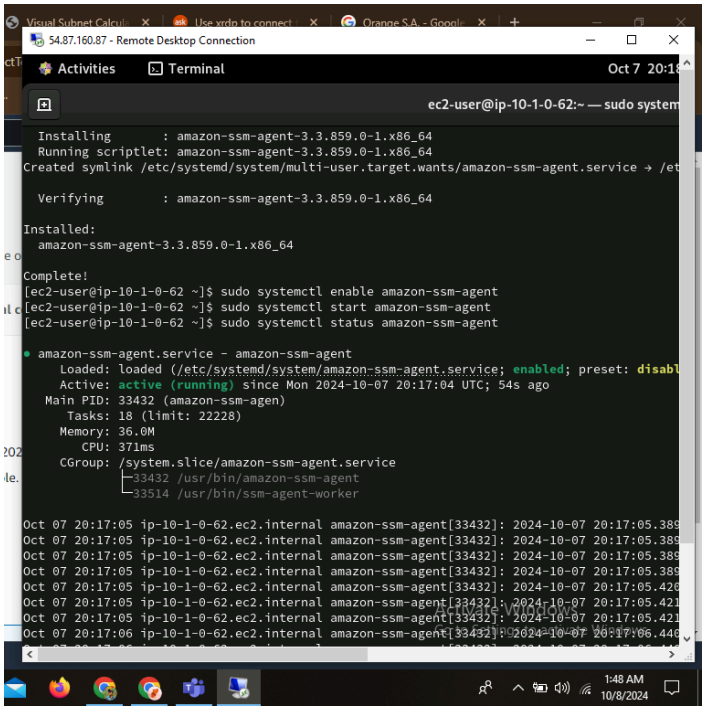
10.3 To check the status of the SSM Agent service type in the command:

```
sudo systemctl status amazon-ssm-agent
```

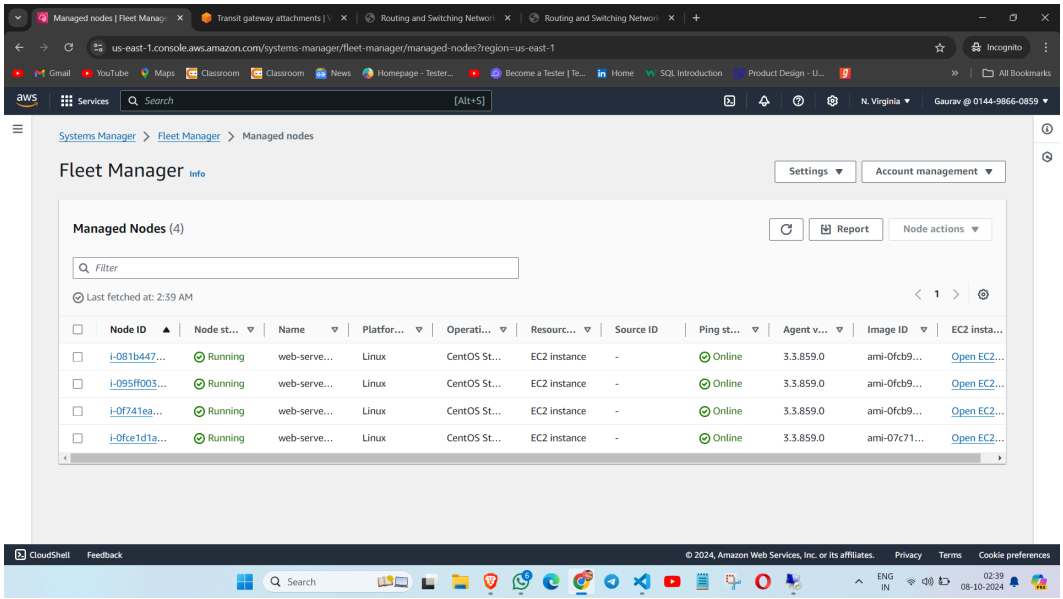


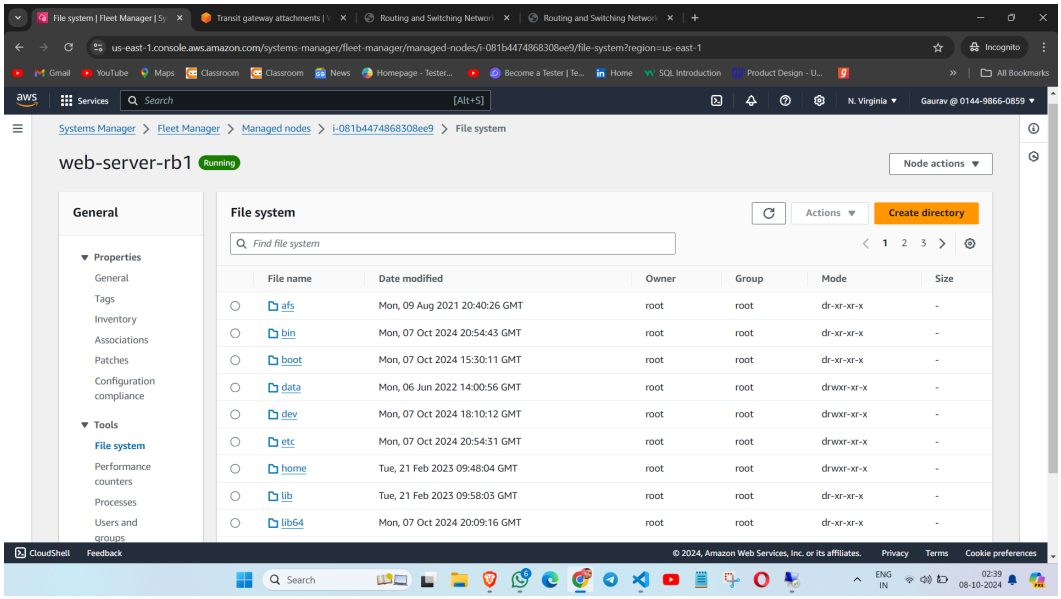
10.4 Now, enable and start the service for that type in the command:

```
sudo systemctl enable amazon-ssm-agent
sudo systemctl start amazon-ssm-agent
```



10.5 Now, go to the Fleet Manager under Node Management to check the files.




File system | Fleet Manager | Sy
Transit gateway attachments | V
Routing and Switching Networ
Routing and Switching Networ
us-east-1.console.aws.amazon.com/systems-manager/fleet-manager/managed-nodes/i-081b4474868308ee9/file-system?region=us-east-1
Incognito
Gmail
YouTube
Maps
Classroom
Classroom
News
Homepage - Tester...
Become a Tester | Te...
Home
SQL Introduction
Product Design - U...
All Bookmarks
aws
Services
Search
[Alt+S]
N. Virginia
Gaurav @ 0144-9866-0859
Systems Manager
Fleet Manager
Managed nodes
i-081b4474868308ee9
File system
web-server-rb1
Running
Node actions
General
Properties
General
Tags
Inventory
Associations
Patches
Configuration compliance
Tools
File system
Performance counters
Processes
Users and groups
File system
Actions
Create directory
Find file system
1
2
3
File name
Date modified
Owner
Group
Mode
Size
afs
Mon, 09 Aug 2021 20:40:26 GMT
root
root
dr-xr-xr-x
-
bin
Mon, 07 Oct 2024 20:54:43 GMT
root
root
dr-xr-xr-x
-
boot
Mon, 07 Oct 2024 15:30:11 GMT
root
root
dr-xr-xr-x
-
data
Mon, 06 Jun 2022 14:00:56 GMT
root
root
drwxr-xr-x
-
dev
Mon, 07 Oct 2024 18:10:12 GMT
root
root
drwxr-xr-x
-
etc
Mon, 07 Oct 2024 20:54:31 GMT
root
root
drwxr-xr-x
-
home
Tue, 21 Feb 2023 09:48:04 GMT
root
root
drwxr-xr-x
-
lib
Tue, 21 Feb 2023 09:58:03 GMT
root
root
dr-xr-xr-x
-
lib64
Mon, 07 Oct 2024 20:09:16 GMT
root
root
dr-xr-xr-x
-
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
IN
02:39
08-10-2024

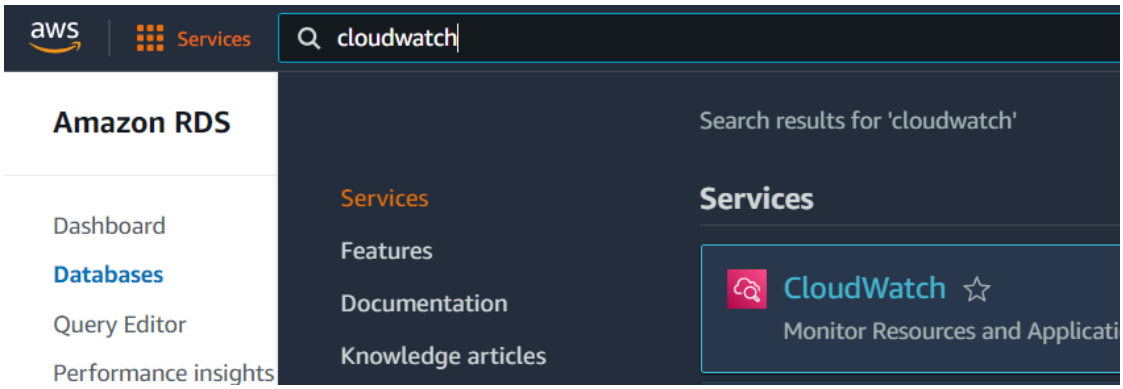
11. CloudWatch Configuration

CloudWatch Configuration:

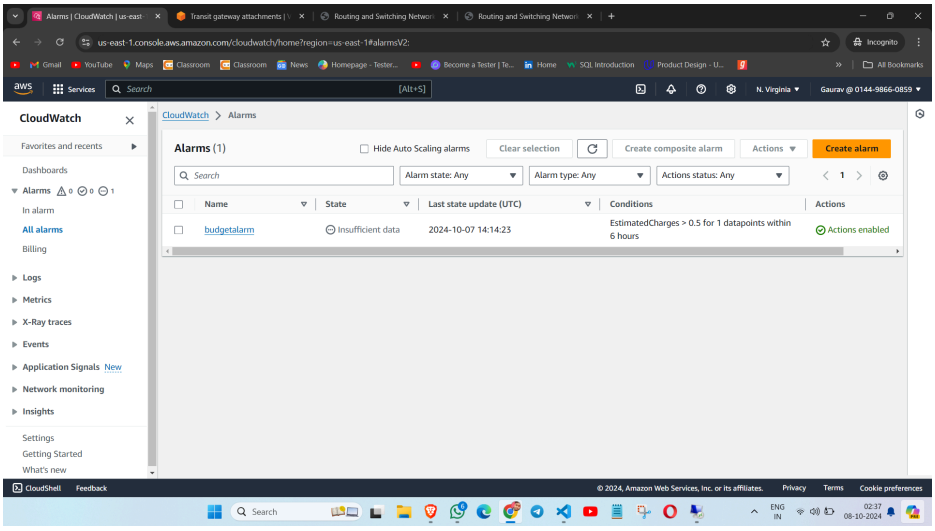
- Create an **Alarm** and choose the metric as Billing and EstimatedCharges and threshold value.
- Create a **Dashboard** and add the widgets to visualize the metrics.
- Create the **Logs** and stream for EC2 instances in the log groups

Step 11: Launch CloudWatch to monitor the Data

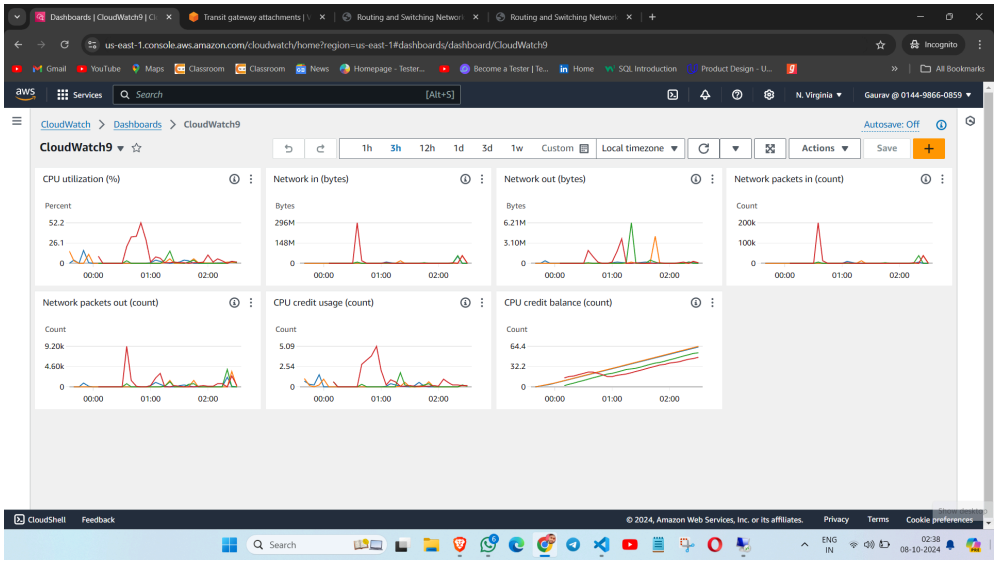
11.1 In Dashboard, search for CloudWatch service, click **CloudWatch** to open it.



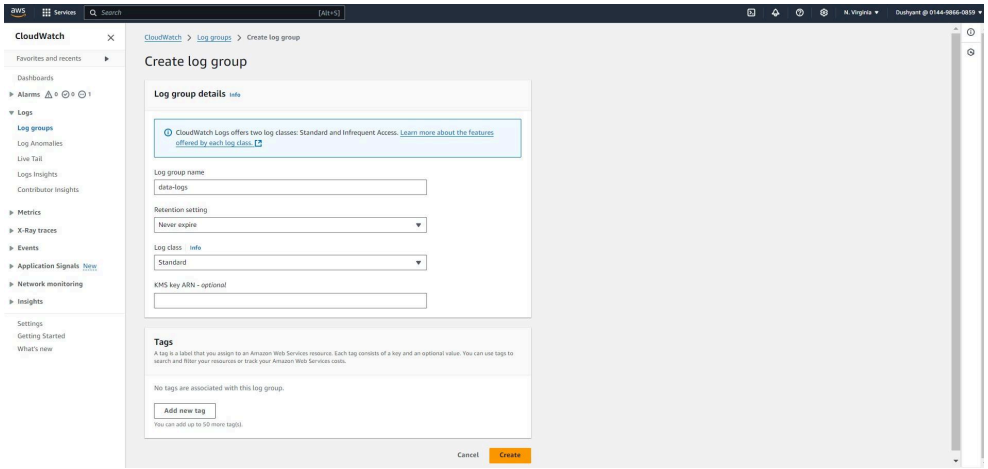
11.2 Create an Alarm and choose the metric as Billing and EstimatedCharges and threshold value.



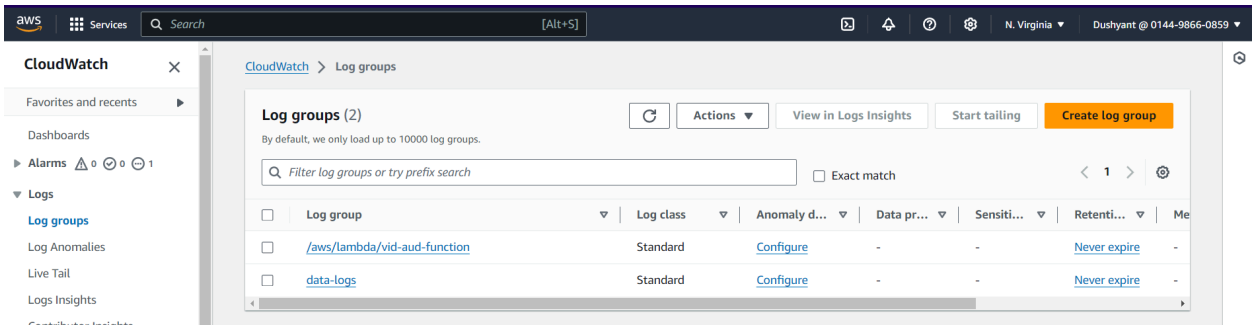
11.3 Create the Dashboard and add the widgets to visualize the metrics.



11.4 Create the Logs and stream for EC2 instances in the log groups.



11.5 Assign the name and associate the metrics, subscription filters.



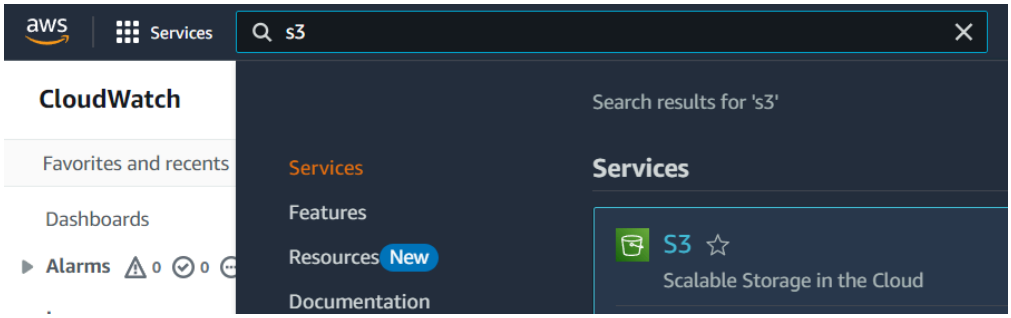
12. S3 Configuration

S3 Configuration:

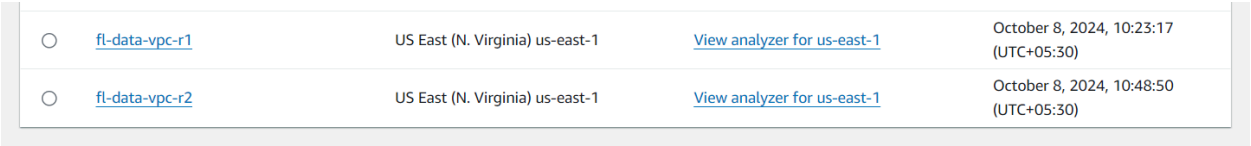
- Create S3 buckets for capturing the flow logs of 2 VPCs.
- Go to the VPC and configure the flow filtering the traffic to ALL.
- Assigning the destination as S3 bucket which we have created.

Step 12: Build VPC Flow logs to S3 Destination

12.1 In Dashboard, search for S3 service, click **S3** to open it.

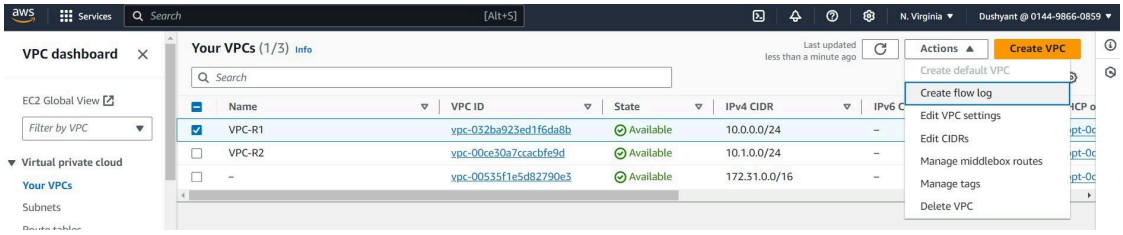


12.2 Create the buckets to feed the data.

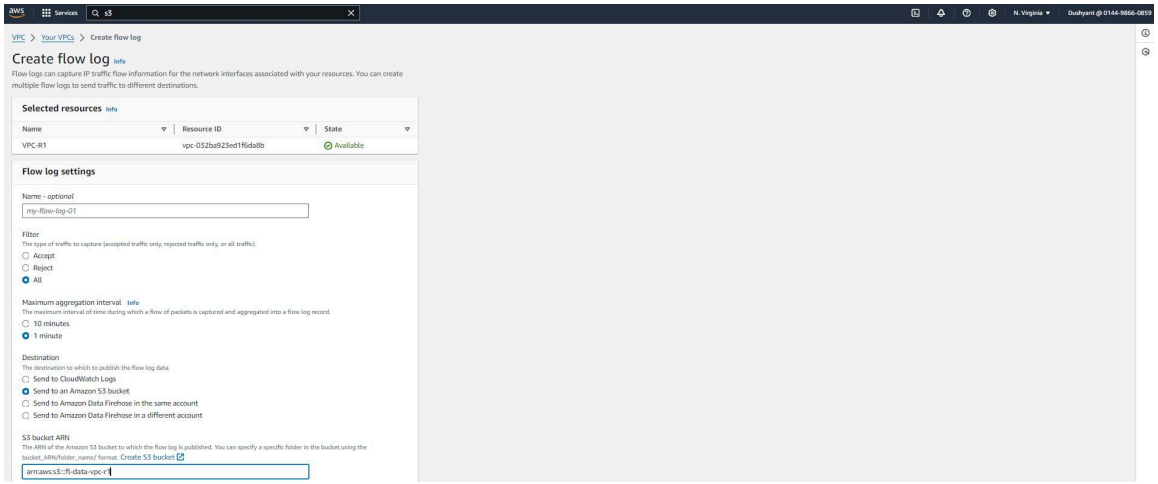


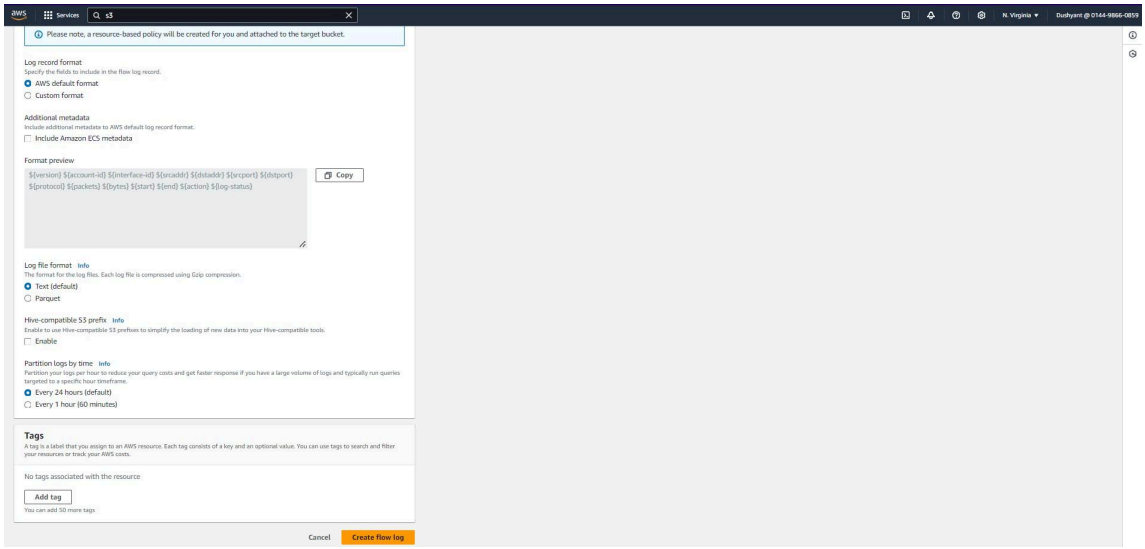
○	fl-data-vpc-r1	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 8, 2024, 10:23:17 (UTC+05:30)
○	fl-data-vpc-r2	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 8, 2024, 10:48:50 (UTC+05:30)

12.3 Go to the VPC and configure the flow filtering the traffic to ALL.

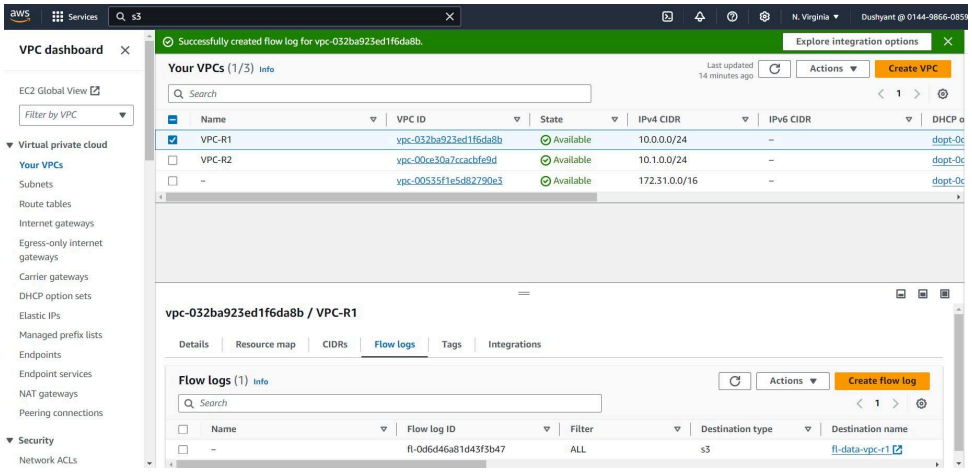


12.4 Add the destination to S3 bucket





12.5 Successfully configured the VPC flow logs with S3 destination.



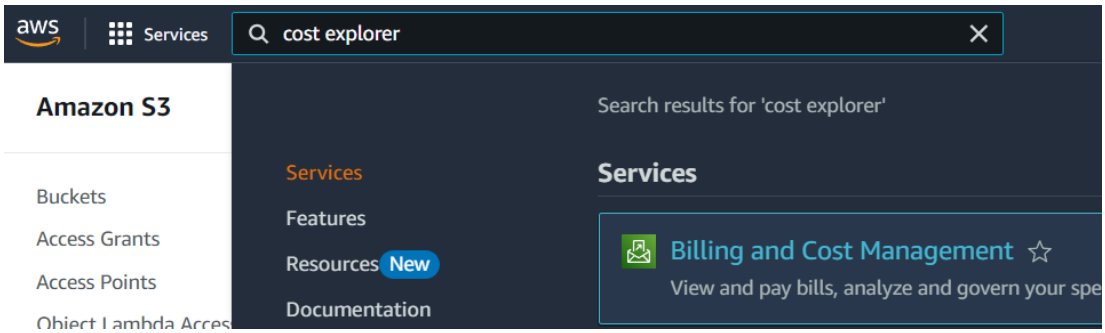
13. Cost Explorer Configuration

Cost Explorer Configuration:

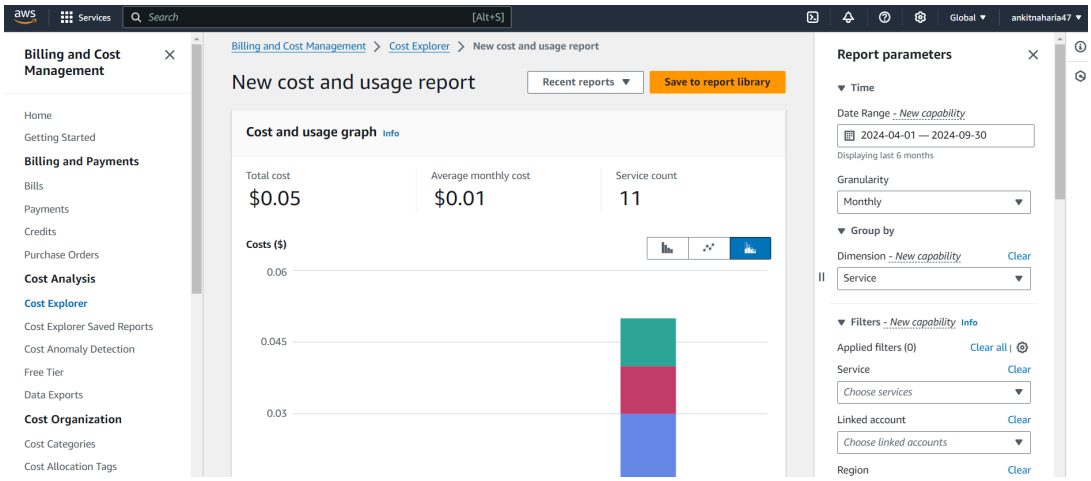
- Go to Cost Explorer and just enable it.
- Once enabled, visualize the cost of daily, cost allocation, service breakdowns.
- Option to to filter the time period and services to analyze.

Step 13: Enable the Cost Explorer in Console

13.1 In Dashboard, search for Cost Explorer service, click **Billing and Cost management** to open it.



13.2 Make a report of it by clicking Save to report library.



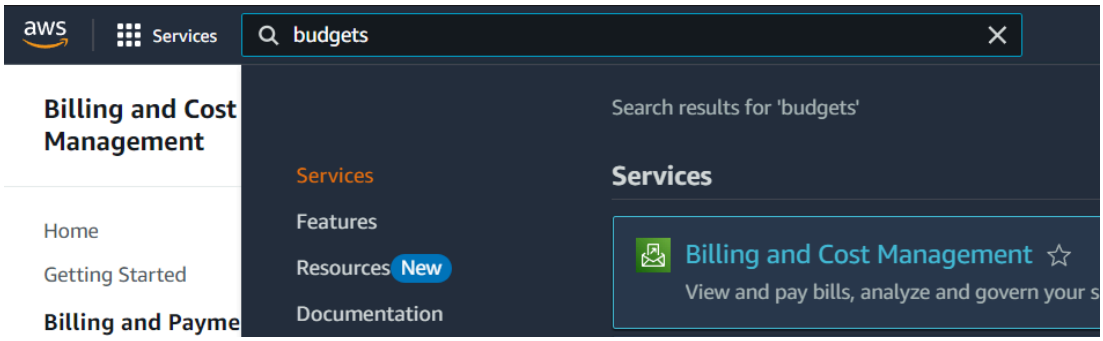
14. Budget Configuration

Budgets Configuration:

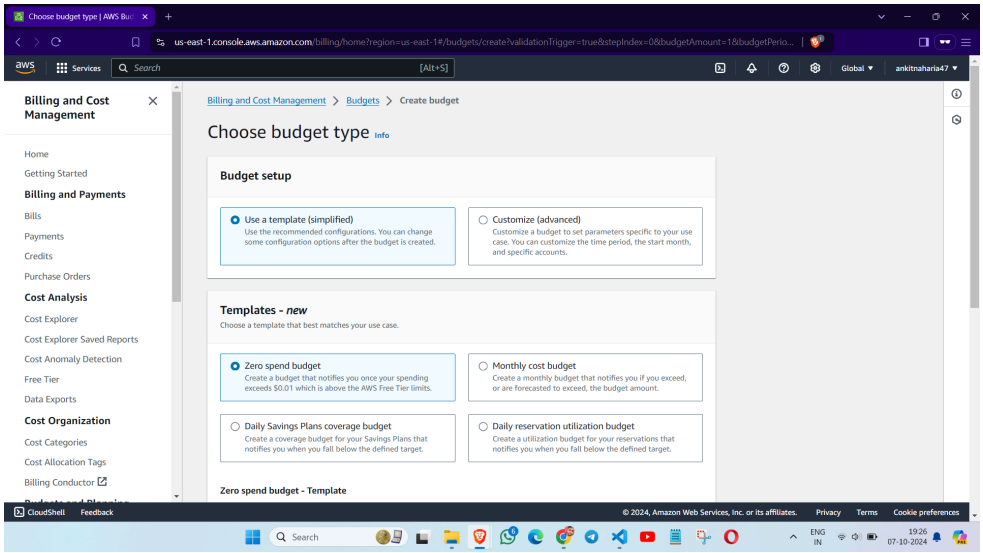
- Click on **Budgets** under the **Billing** section, select the Cost budget type and budget period monthly.
- Similarly create one more Budget for Savings plan budget type and budget period daily.

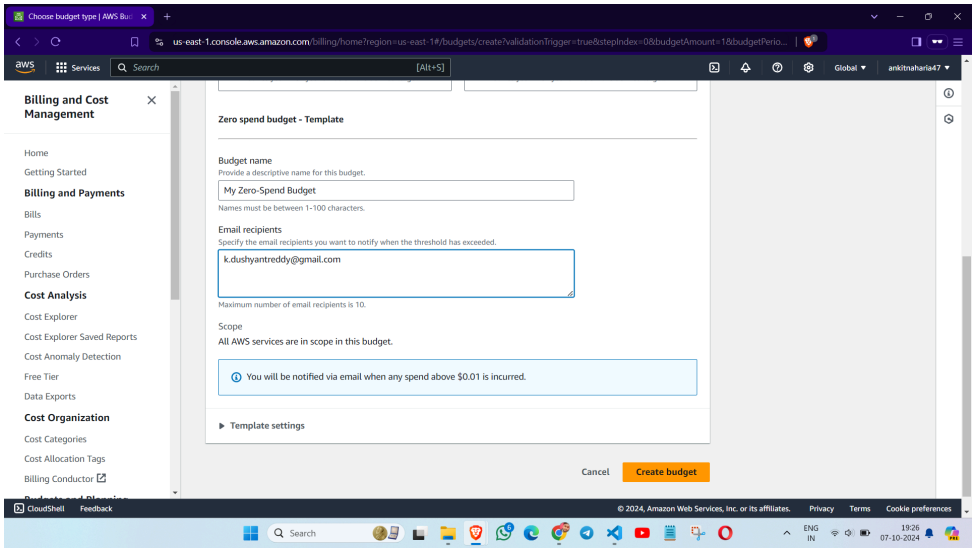
Step 14: Allotting the Budget in Console

14.1 In Dashboard, search for Budgets service, click **Billing and Cost management** to open it.

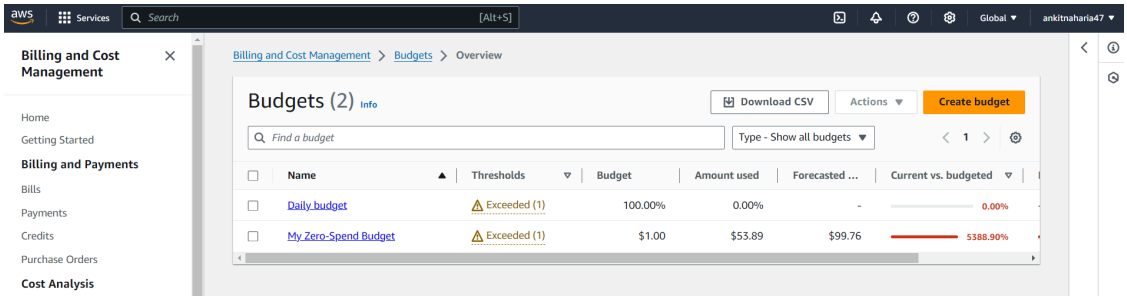


14.2 Choose the Budget type and add the email ID to confirm.

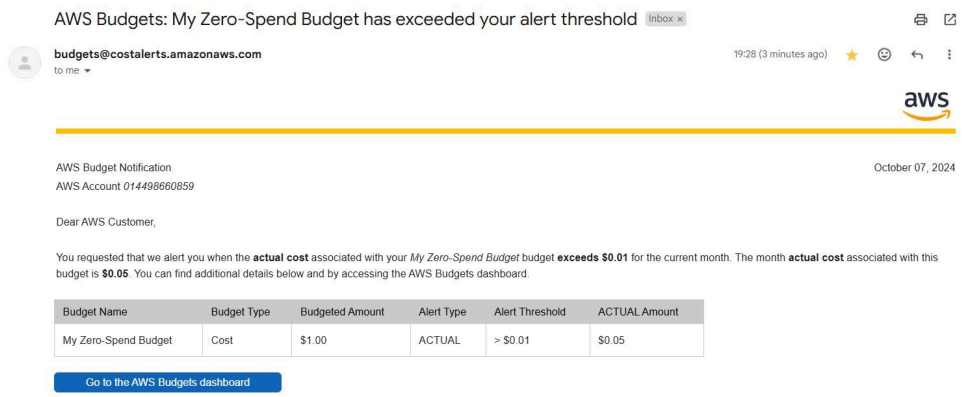




14.3 Create one more Budget of type Daily budget.



14.4 Received the mail for exceeding the threshold



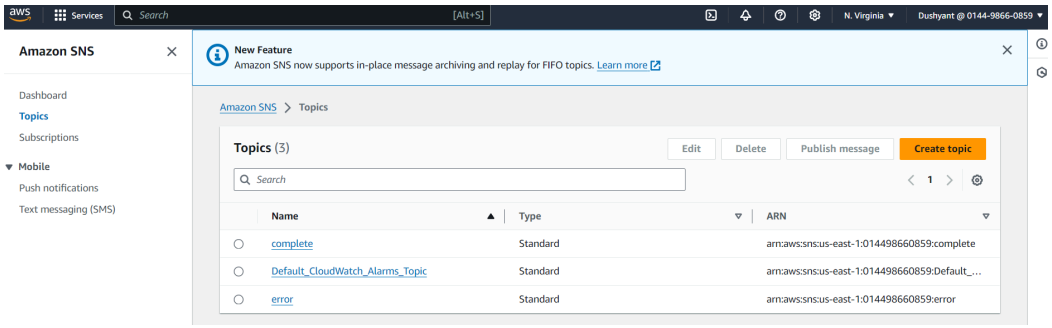
15. SNS Configuration

SNS Configuration:

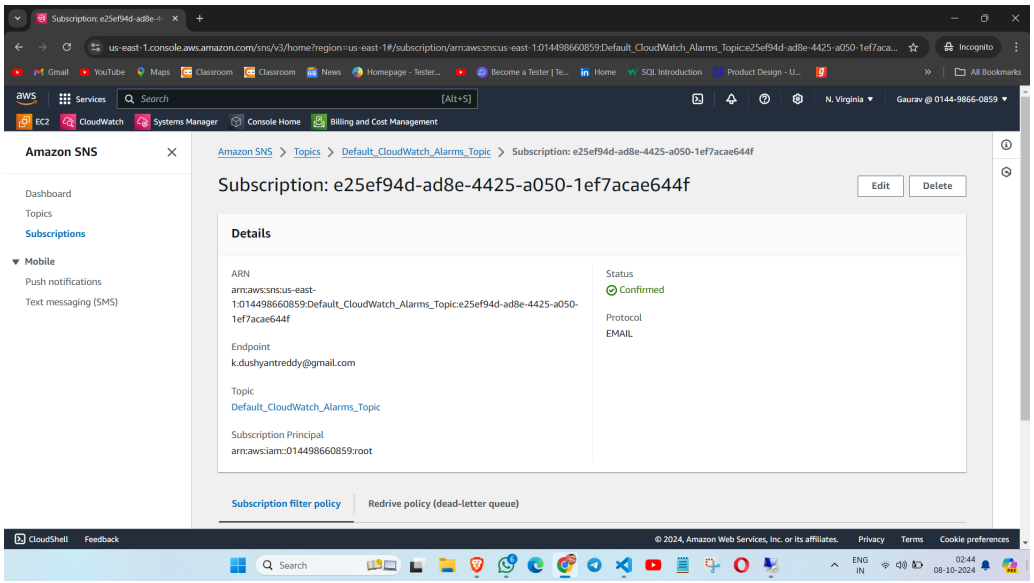
- Navigate to **SNS**, create a Topic of standard type and assign a name for it.
- Go to CloudWatch alarms under Notification choose the SNS topic which you have created and configure via email.

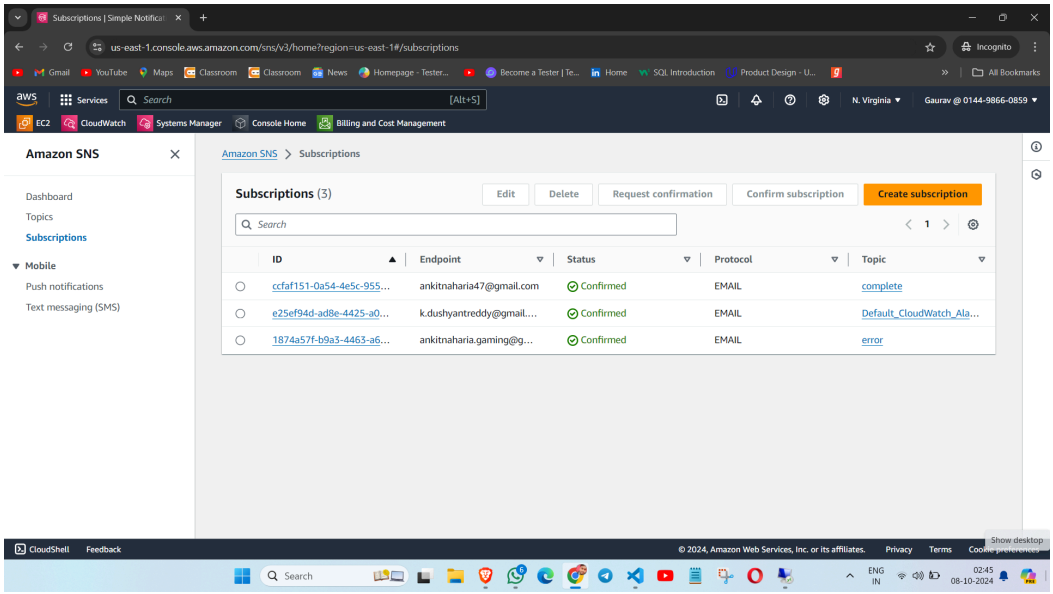
Step 15: Build CloudWatch Alarm subscribed to SNS Email

15.1 Create a Topic of standard type named '**Default_CloudWatch_Alarm_Topic**'.

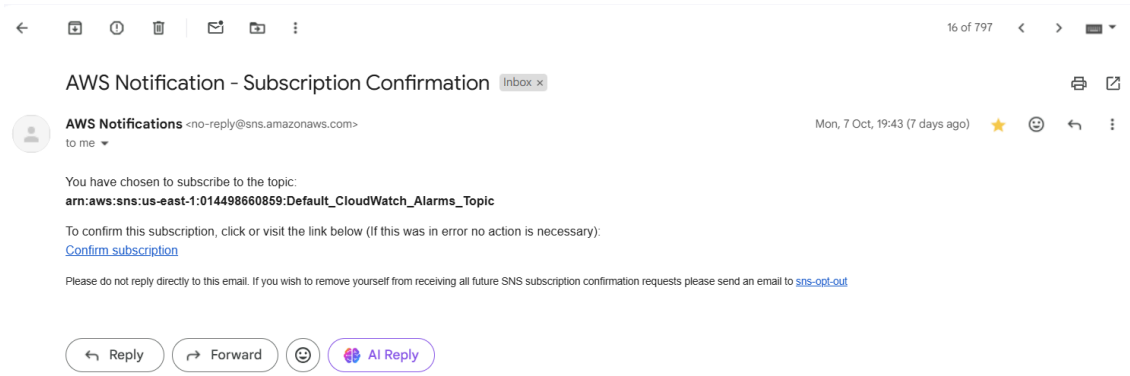


15.2 Create the Subscription of the assigning the Email to get the notification.





15.3 Received the confirmation mail to subscribe.



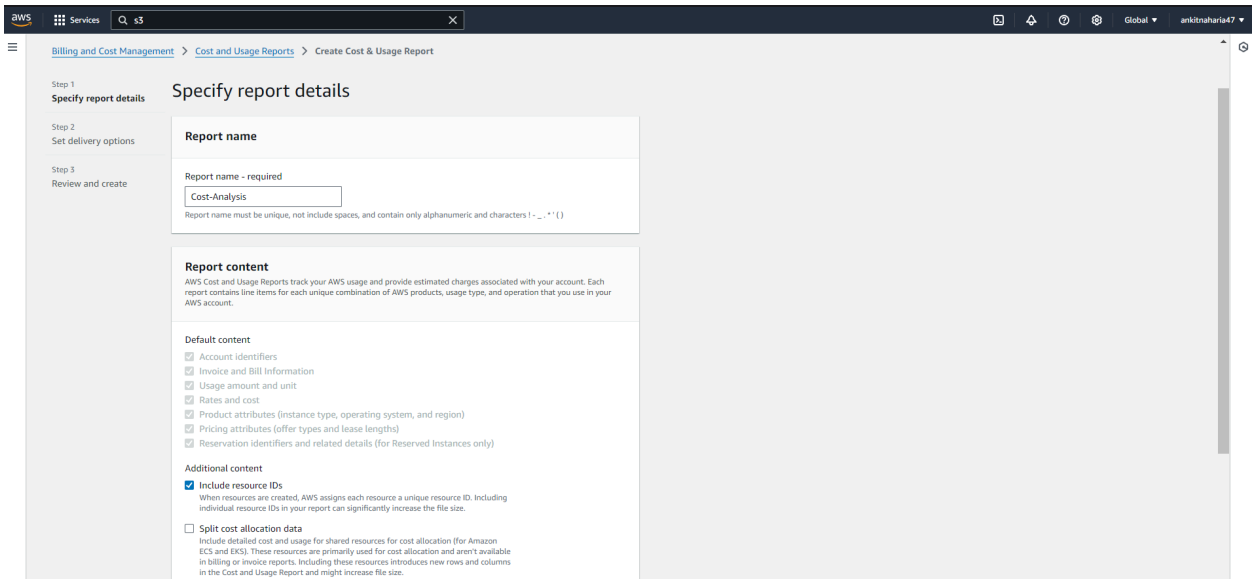
16. Cost and Usage Report Configuration

Cost and Usage Report Configuration:

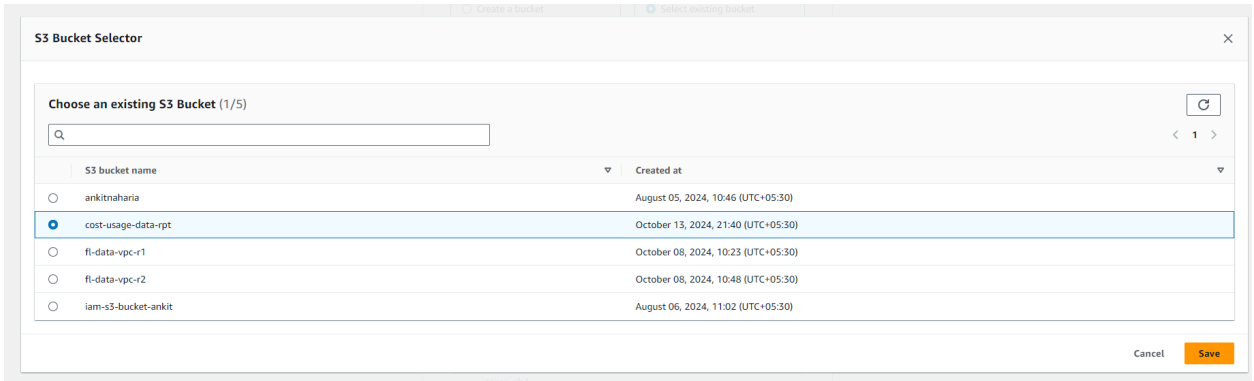
- Click on **Cost Management** and create a new report and assign a name.
- Configure the resource IDs and add the S3 destination and click Create Report.

Step 16: Build Report to S3 Destination

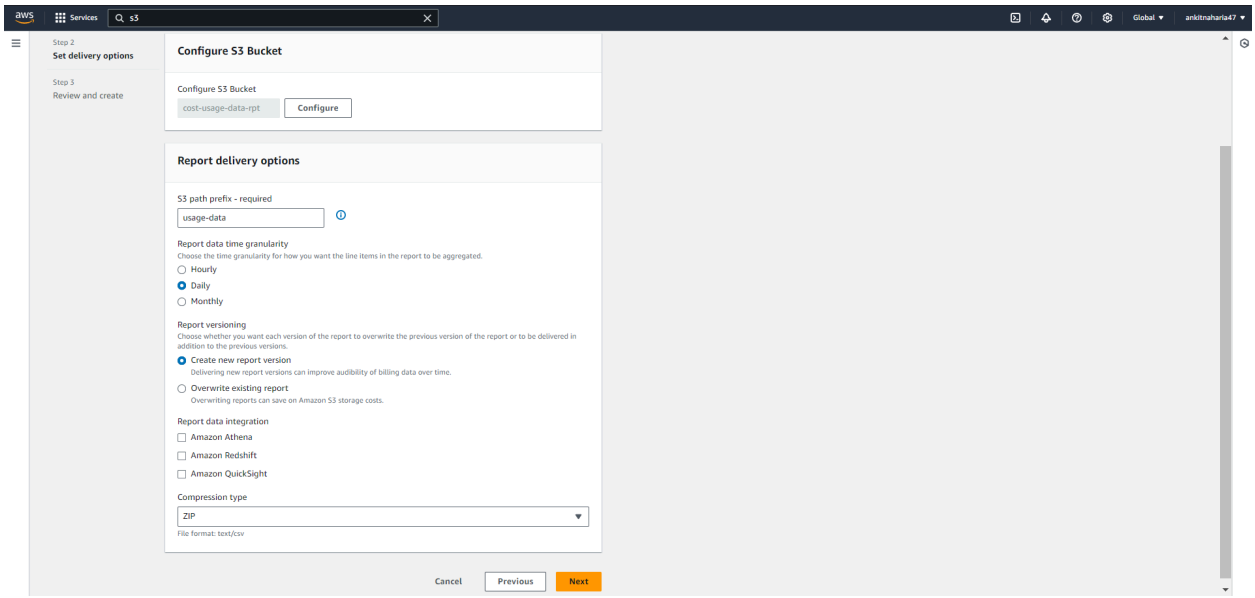
16.1 Create Cost and Usage Report with report name and adding the Resource IDs.

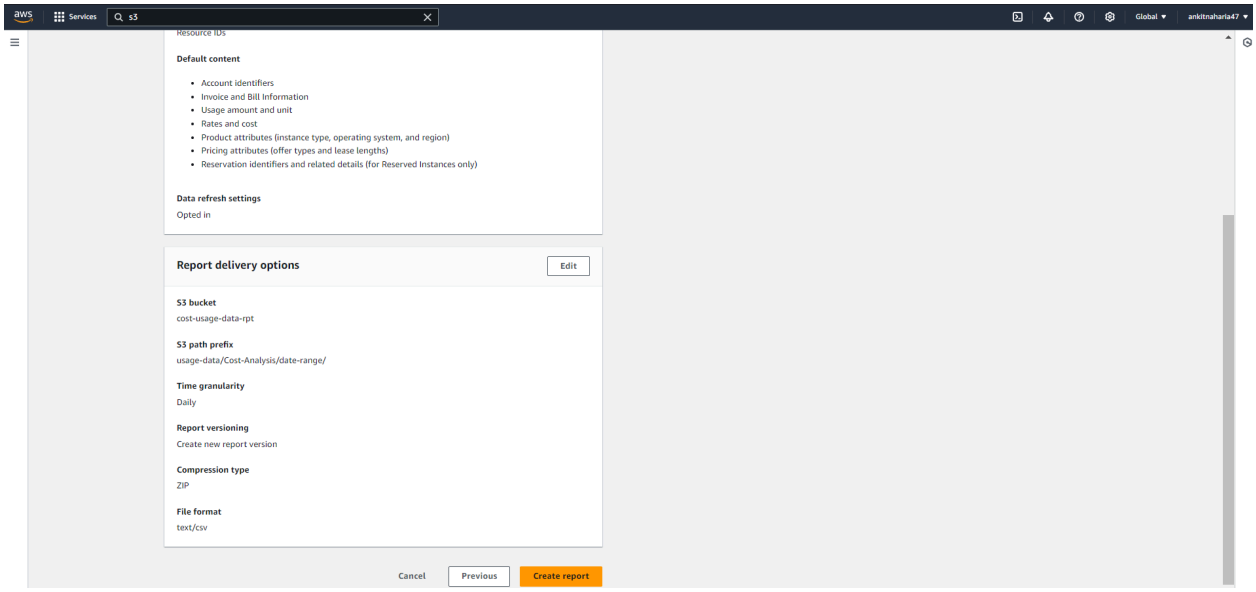


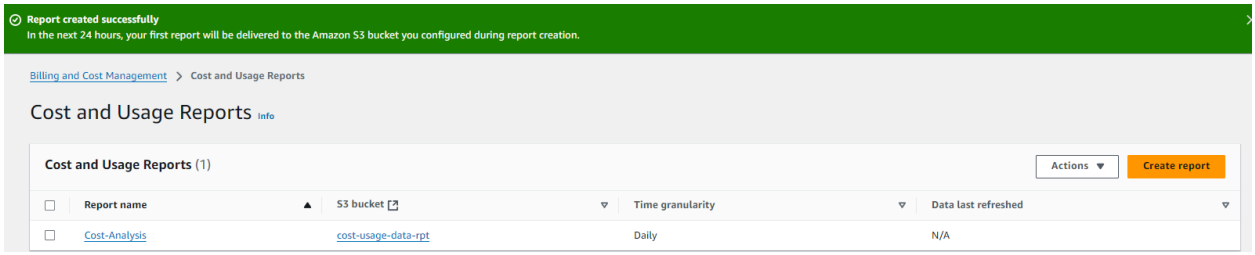
16.2 Configure S3 bucket by choosing the selector of the existing bucket and click Save.



16.3 Click Next and review the details and click Create report.



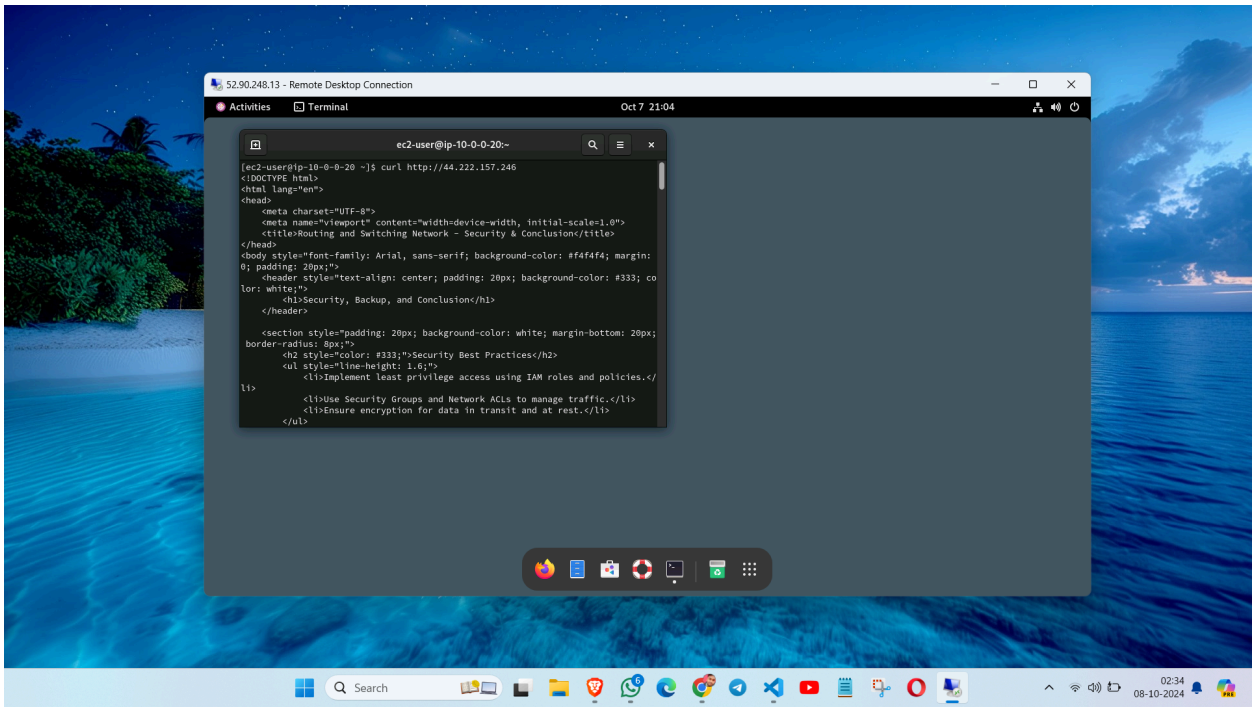


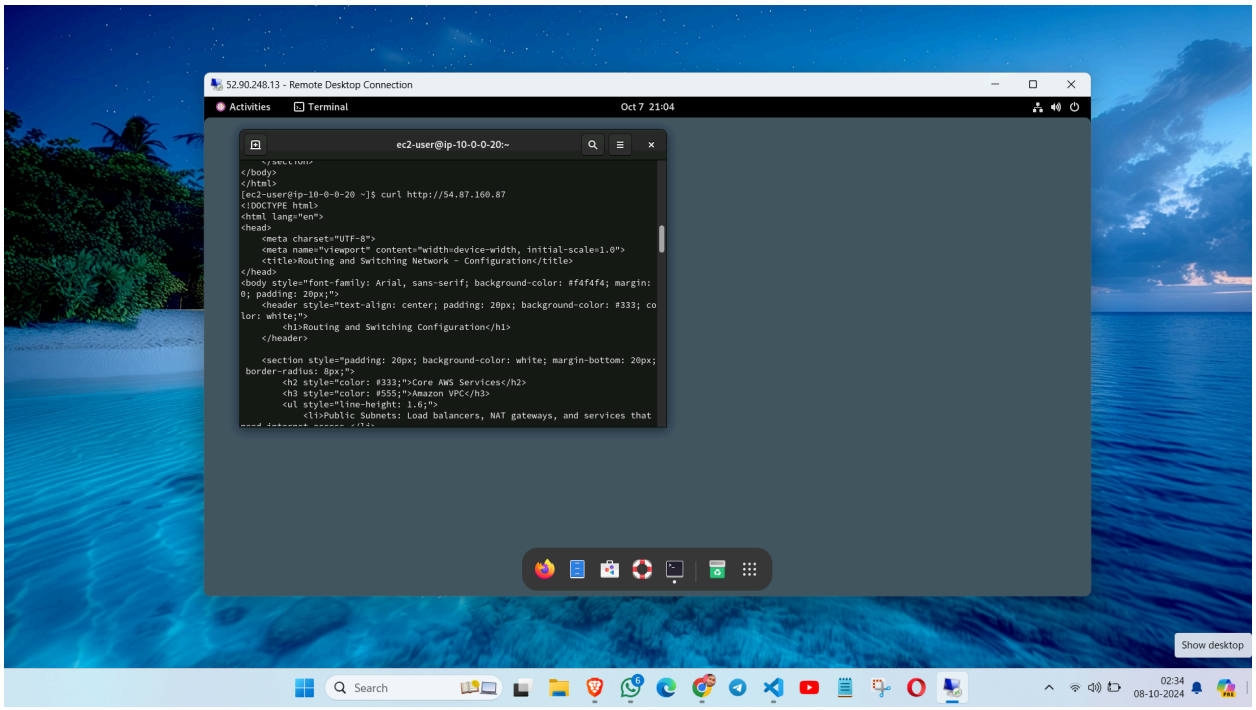


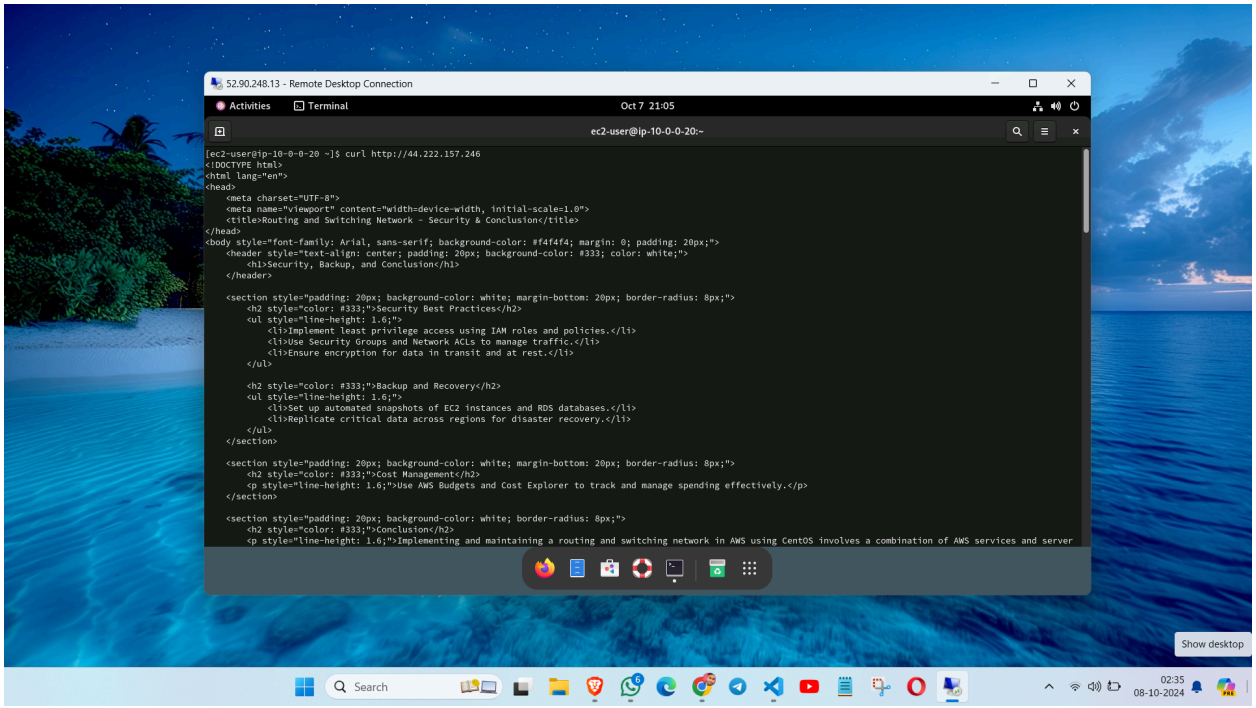
PROJECT OUTPUT

In this project, we have configured the switching and routing through:

Ping VPCs

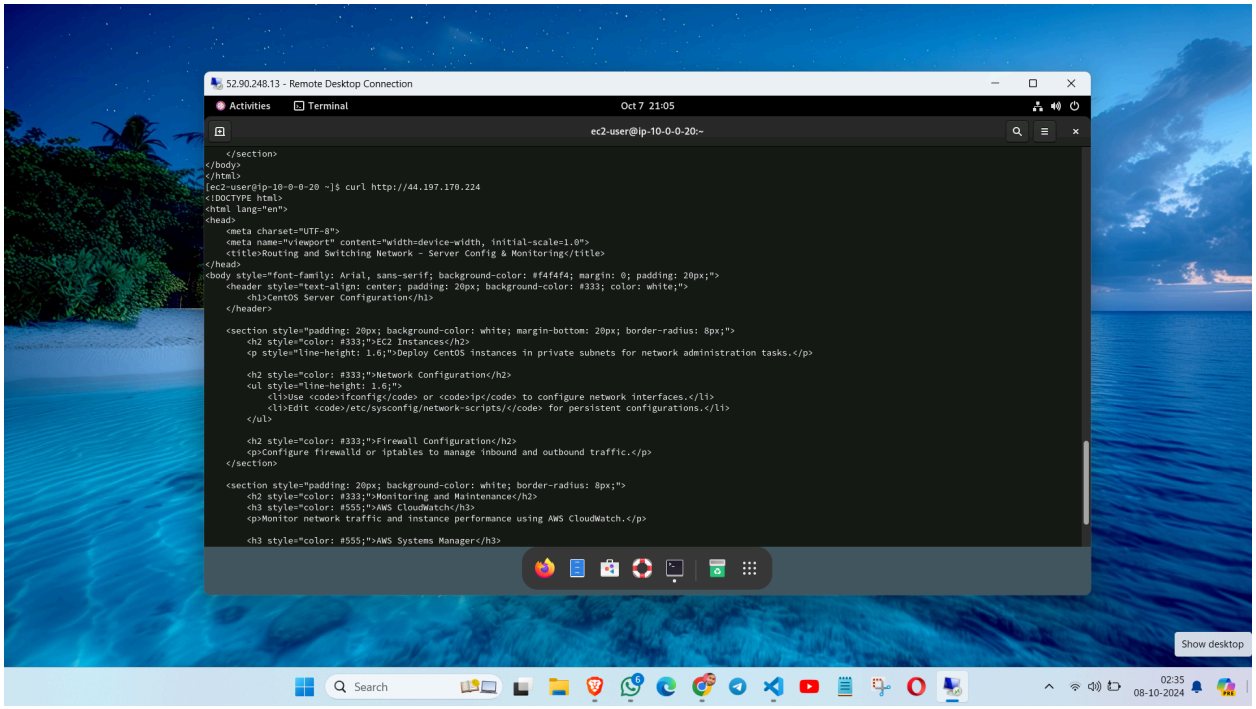





52.90.248.13 - Remote Desktop Connection
Activities
Terminal
Oct 7 21:05
ec2-user@ip-10-0-0-20:~
[ec2-user@ip-10-0-0-20 ~]$ curl http://44.222.157.246
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>Routing and Switching Network - Security & Conclusion</title>
</head>
<body style="font-family: Arial, sans-serif; background-color: #f4f4f4; margin: 0; padding: 20px;">
<header style="text-align: center; padding: 20px; background-color: #333; color: white;">
<h1>Security, Backup, and Conclusion</h1>
</header>
<section style="padding: 20px; background-color: white; margin-bottom: 20px; border-radius: 8px;">
<h2 style="color: #333;">Security Best Practices</h2>
<ul style="line-height: 1.6;">
Implement least privilege access using IAM roles and policies.
Use Security Groups and Network ACLs to manage traffic.
Ensure encryption for data in transit and at rest.

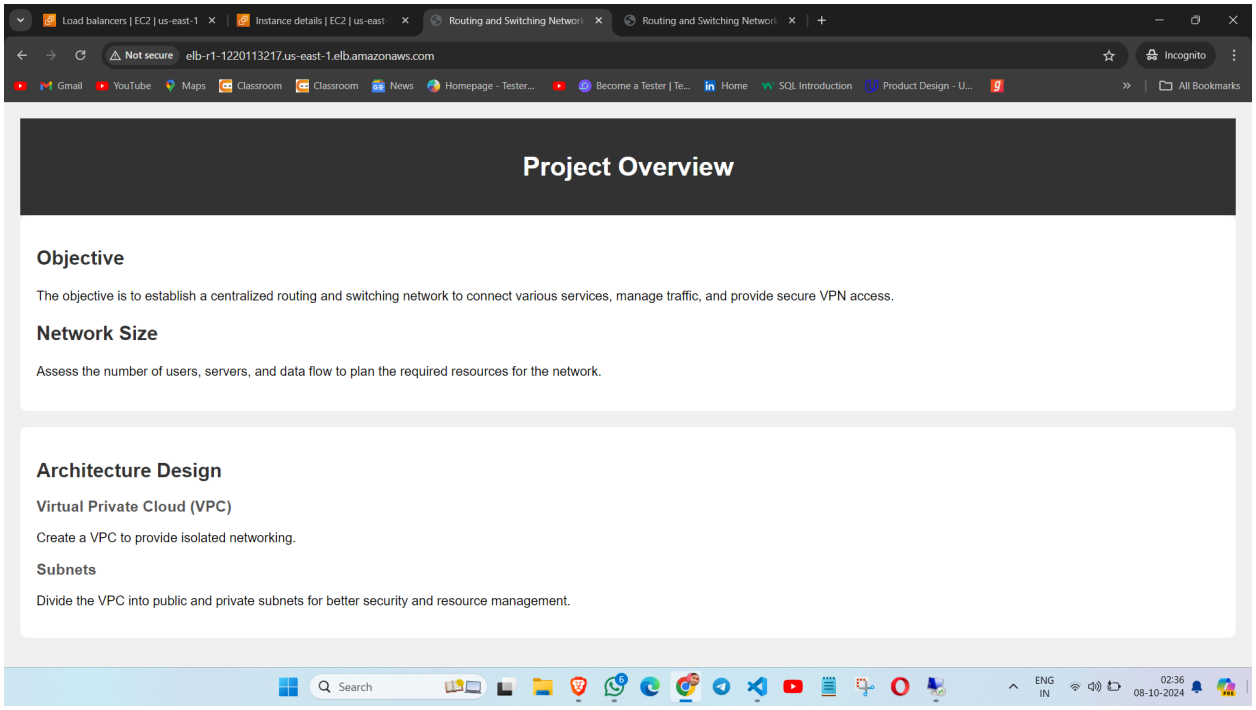
<h2 style="color: #333;">Backup and Recovery</h2>
<ul style="line-height: 1.6;">
Set up automated snapshots of EC2 instances and RDS databases.
Replicate critical data across regions for disaster recovery.

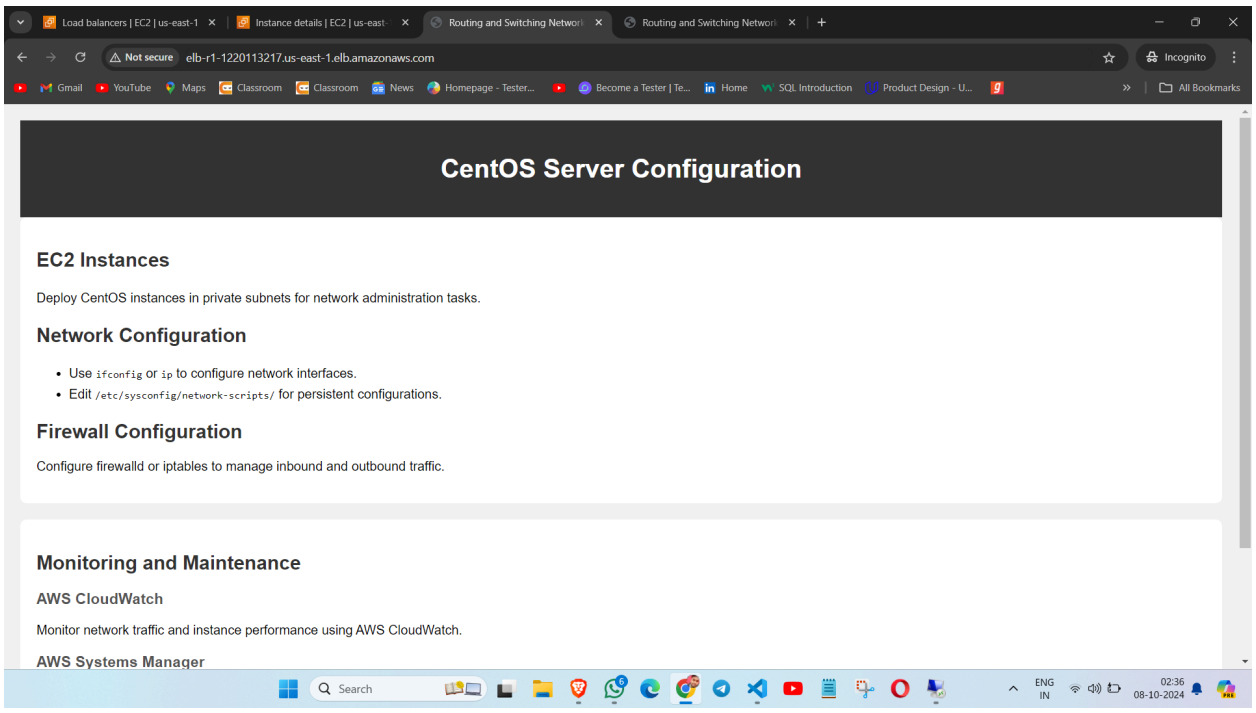
</section>
<section style="padding: 20px; background-color: white; margin-bottom: 20px; border-radius: 8px;">
<h2 style="color: #333;">Cost Management</h2>
Use AWS Budgets and Cost Explorer to track and manage spending effectively.
</section>
<section style="padding: 20px; background-color: white; border-radius: 8px;">
<h2 style="color: #333;">Conclusion</h2>
Implementing and maintaining a routing and switching network in AWS using CentOS involves a combination of AWS services and server
Show desktop
Search
02:35
08-10-2024

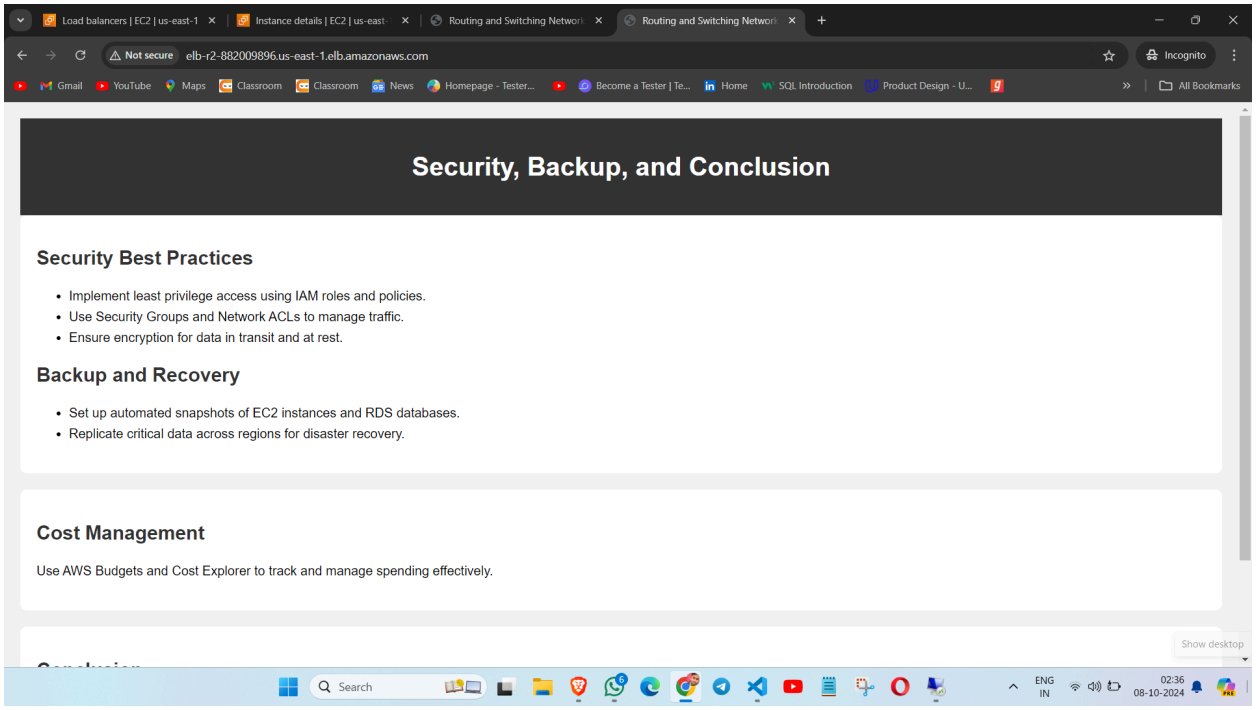

52.90.248.13 - Remote Desktop Connection
Activities
Terminal
Oct 7 21:05
ec2-user@ip-10-0-0-20:~
</section>
</body>
</html>
[ec2-user@ip-10-0-0-20 ~]$ curl http://44.197.170.224
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>Routing and Switching Network - Server Config & Monitoring</title>
</head>
<body style="font-family: Arial, sans-serif; background-color: #f4f4f4; margin: 0; padding: 20px;">
<header style="text-align: center; padding: 20px; background-color: #333; color: white;">
<h1>CentOS Server Configuration</h1>
</header>
<section style="padding: 20px; background-color: white; margin-bottom: 20px; border-radius: 8px;">
<h2 style="color: #333;">EC2 Instances</h2>
Deploy CentOS instances in private subnets for network administration tasks.
<h2 style="color: #333;">Network Configuration</h2>
<ul style="line-height: 1.6;">
Use <code>ifconfig</code> or <code>ip</code> to configure network interfaces.
Edit <code>/etc/sysconfig/network-scripts/</code> for persistent configurations.

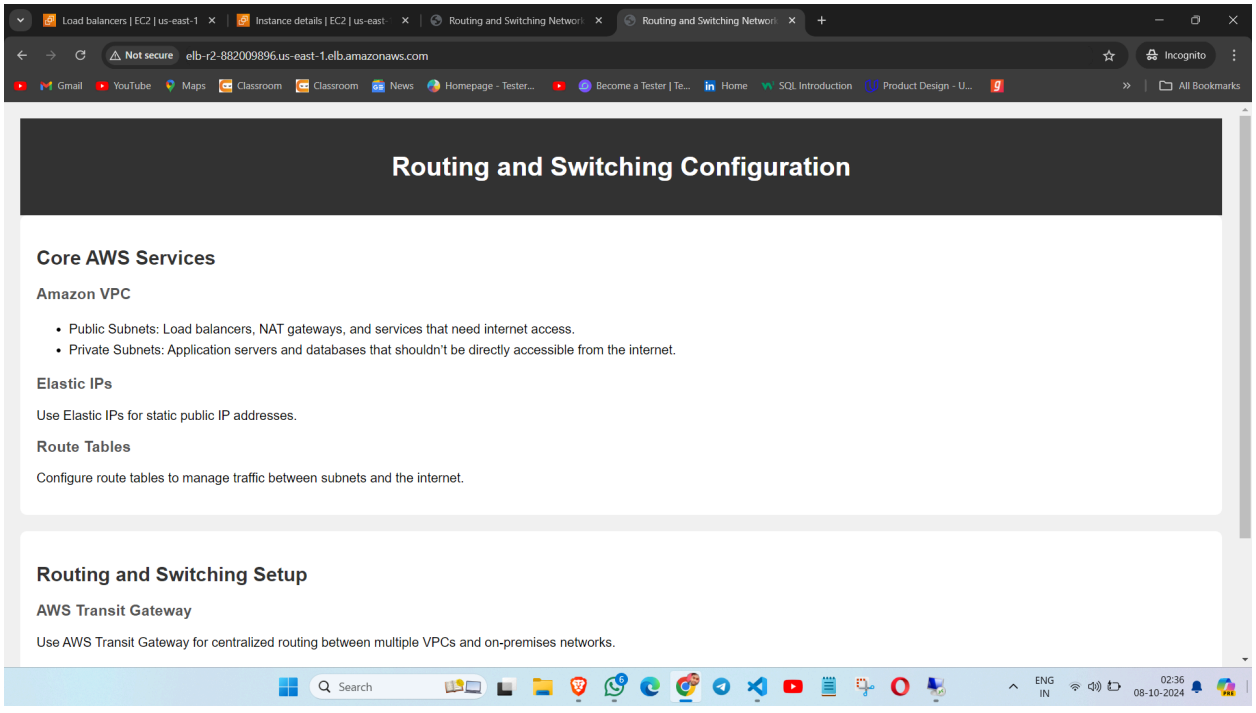
<h2 style="color: #333;">Firewall Configuration</h2>
Configure firewalld or iptables to manage inbound and outbound traffic.
</section>
<section style="padding: 20px; background-color: white; border-radius: 8px;">
<h2 style="color: #333;">Monitoring and Maintenance</h2>
<h3 style="color: #555;">AWS CloudWatch</h3>
Monitor network traffic and instance performance using AWS CloudWatch.
<h3 style="color: #555;">AWS Systems Manager</h3>
Show desktop
Search
02:35
08-10-2024

Web Pages


Load balancers | EC2 | us-east-1
Instance details | EC2 | us-east-
Routing and Switching Networ
Routing and Switching Networ
Not secure
elb-r1-1220113217.us-east-1.elb.amazonaws.com
Incognito
Gmail
YouTube
Maps
Classroom
Classroom
News
Homepage - Tester...
Become a Tester | Te...
Home
SQL Introduction
Product Design - U...
All Bookmarks
Project Overview
Objective
The objective is to establish a centralized routing and switching network to connect various services, manage traffic, and provide secure VPN access.
Network Size
Assess the number of users, servers, and data flow to plan the required resources for the network.
Architecture Design
Virtual Private Cloud (VPC)
Create a VPC to provide isolated networking.
Subnets
Divide the VPC into public and private subnets for better security and resource management.
Search
ENG
IN
02:36
08-10-2024


Load balancers | EC2 | us-east-1
Instance details | EC2 | us-east-
Routing and Switching Networ
Routing and Switching Networ
Not secure
elb-r1-1220113217.us-east-1.elb.amazonaws.com
Incognito
Gmail
YouTube
Maps
Classroom
Classroom
News
Homepage - Tester...
Become a Tester | Te...
Home
SQL Introduction
Product Design - U...
All Bookmarks
CentOS Server Configuration
EC2 Instances
Deploy CentOS instances in private subnets for network administration tasks.
Network Configuration
Use ifconfig or ip to configure network interfaces.
Edit /etc/sysconfig/network-scripts/ for persistent configurations.
Firewall Configuration
Configure firewalld or iptables to manage inbound and outbound traffic.
Monitoring and Maintenance
AWS CloudWatch
Monitor network traffic and instance performance using AWS CloudWatch.
AWS Systems Manager
Search
ENG
IN
02:36
08-10-2024


Load balancers | EC2 | us-east-1
Instance details | EC2 | us-east-
Routing and Switching Networ
Routing and Switching Networ
Not secure
elb-r2-882009896.us-east-1.elb.amazonaws.com
Incognito
Gmail
YouTube
Maps
Classroom
Classroom
News
Homepage - Tester...
Become a Tester | Te...
Home
SQL Introduction
Product Design - U...
All Bookmarks
Security, Backup, and Conclusion
Security Best Practices
Implement least privilege access using IAM roles and policies.
Use Security Groups and Network ACLs to manage traffic.
Ensure encryption for data in transit and at rest.
Backup and Recovery
Set up automated snapshots of EC2 instances and RDS databases.
Replicate critical data across regions for disaster recovery.
Cost Management
Use AWS Budgets and Cost Explorer to track and manage spending effectively.
Show desktop
Search
ENG
IN
02:36
08-10-2024


Load balancers | EC2 | us-east-1
Instance details | EC2 | us-east-
Routing and Switching Networ
Routing and Switching Networ
Not secure
elb-r2-882009896.us-east-1.elb.amazonaws.com
Incognito
Gmail
YouTube
Maps
Classroom
Classroom
News
Homepage - Tester...
Become a Tester | Te...
Home
SQL Introduction
Product Design - U...
All Bookmarks
Routing and Switching Configuration
Core AWS Services
Amazon VPC
Public Subnets: Load balancers, NAT gateways, and services that need internet access.
Private Subnets: Application servers and databases that shouldn't be directly accessible from the internet.
Elastic IPs
Use Elastic IPs for static public IP addresses.
Route Tables
Configure route tables to manage traffic between subnets and the internet.
Routing and Switching Setup
AWS Transit Gateway
Use AWS Transit Gateway for centralized routing between multiple VPCs and on-premises networks.
Search
ENG
IN
02:36
08-10-2024

FUTURE SCOPE

The future goals of this project can evolve to address changing business requirements, adopt new technologies, and maintain a competitive edge while ensuring a stable and scalable network infrastructure.

Future Goals for the Centralized Network:

- **Global Expansion:** Extend the network to new regions for better performance and international reach.
- **Enhanced Security:** Integrate advanced security tools and automate compliance checks.
- **Cost Optimization:** Utilize cost-monitoring tools and automate resource scheduling.
- **AI Integration:** Leverage machine learning for traffic analysis, anomaly detection, and predictive scaling.
- **Automated Response:** Implement self-healing infrastructure and automated incident handling.
- **Hybrid and Multi-Cloud Support:** Expand to support hybrid environments with seamless cloud integrations.
- **Monitoring Improvements:** Enhance monitoring and logging for better issue detection.
- **DevOps Support:** Automate deployments and updates through CI/CD and infrastructure-as-code.

These goals aim to enhance scalability, security, and cost-efficiency while supporting future growth.

CONCLUSION

In conclusion, the project's implementation of a secure, scalable, and highly available network infrastructure in AWS using CentOS provides a robust foundation for supporting a centralized large network. The architecture not only ensures optimal performance, security, and cost-efficiency but also facilitates rapid fault detection and resolution to minimize downtime. With strategies for future growth, including scaling, enhanced segmentation, integration of new services, and global expansion, the network is well-equipped to adapt to evolving business needs and traffic demands. This approach ensures long-term sustainability, enabling the organization to efficiently manage current operations while seamlessly accommodating future growth.This project helps mitigate real-time issues by providing rapid fault detection, minimizing downtime, and enabling quick recovery from failures, thus maintaining network performance and security.