# BLACKBUCKS INTERNSHIP REPORT

**An Architecture of AWS – VPC – Subnetting – Auditing - Monitoring**

**SUBMITTED BY**


**Mr. PYDAM NAIDU KALLEMPUDI** **RegdNo:21B91A5719**

**Mr. DEVA YADHALA** **RegdNo:21B91A5763**

**Mr. NAVEEN GOCHIPATHA** **RegdNo:21B91A5713**


**UNDER THE GUIDANCE OF MR. AASHU DEV**

B Tech, AWS solution Architect (2X) certified,

AWS Academy Accredited Educator

**Blackbuck Engineers Pvt, Ltd**

**Road No 36, Jubilee Hills, Hyderabad**

# BLACKBUCK INTERNSHIP WORK

## Team Members:


- PYDAM NAIDU KALLEMPUDI (21B91A5719)
- DEVA YADHALA (21B91A5763)
- NAVEEN GOCHIPATHA (21B91A5713)


## Title:

AWS architecture of **AWS – VPC – Subnetting – Auditing – Monitoring**

## Abstract:


This project demonstrates the creation of a robust AWS architectural infrastructure. Utilizing Amazon VPC with 20 subnets, CloudTrail for auditing, and CloudWatch for monitoring, the system ensures security, scalability, and fault tolerance. The setup includes a bastion host for secure EC2 instance access and Auto Scaling for maintaining optimal capacity. This report offers valuable insights and guidelines for building efficient AWS-based infrastructures

# Table of Contents

## Introduction To Amazon Web Services (AWS):

- **Amazon Web Services, Inc. (AWS)** is a subsidiary of Amazon that provides ondemand cloud computing platforms and APIs to individuals, companies, and governments, on a metered, pay-as-you-go basis. Oftentimes, clients will use this in combination with autoscaling (a process that allows a client to use more computing in times of high application usage, and then scale down to reduce costs when there is less traffic). These cloud computing web services provide various services related to networking, compute, storage, middleware, IoT and other processing capacity, as well as software tools via AWS server farms. This frees clients from managing, scaling, and patching hardware and operating systems. One of the foundational services is Amazon Elastic Compute Cloud (EC2), which allows users to have at their disposal a virtual cluster of computers, with extremely high availability, which can be interacted with over the internet via REST APIs, a CLI or the AWS console. AWS's virtual computers emulate most of the attributes of a real computer, including hardware central processing units (CPUs) and graphics processing units (GPUs) for processing; local/RAM memory; hard-disk/SSD storage; a choice of operating systems; networking; and pre-loaded application software such as web servers, databases, and customer relationship management (CRM)

- AWS services are delivered to customers via a network of AWS server farms located throughout the world. Fees are based on a combination of usage (known as a "Pay-as-yougo" model), hardware, operating system, software, or networking features chosen by the subscriber required availability, redundancy, security, and service options. Subscribers can pay for a single virtual AWS computer, a dedicated physical computer, or clusters of either. Amazon provides select portions of security for subscribers (e.g., physical security of the data centers) while other aspects of security are the responsibility of the subscriber (e.g., account management, vulnerability scanning, patching). AWS operates in many global geographical regions including seven in North America

- Amazon markets AWS to subscribers as a way of obtaining large-scale computing capacity more quickly and cheaply than building an actual physical server farm. All services are billed based on usage, but each service measures usage in varying ways. As of 2021 Q4, AWS has 33% market share for cloud infrastructure while the next two competitors Microsoft Azure and Google Cloud have 21%, and 10% respectively, according to Synergy Group.

## Uses of AWS:

- ✓ A small manufacturing organization uses their expertise to expand their business by leaving their IT management to the AWS.
- ✓ A large enterprise spread across the globe can utilize the AWS to deliver the training to the distributed workforce.
- ✓ An architecture consulting company can use AWS to get the high compute rendering of construction prototype.
- ✓ A media company can use the AWS to provide different types of content such as ebox or audio files to the worldwide files.

## WHY AWS?

There are several reasons why AWS has become a popular choice for cloud computing:

1. Broad and Comprehensive Service Offering: AWS offers a wide range of services to meet various computing needs. Whether you require computer power, storage, databases, machine learning, analytics, networking, or other capabilities, AWS provides a comprehensive set of services to fulfill these requirements.
2. Scalability and Flexibility: AWS allows users to scale their resources up or down based on demand. Whether you need to handle a sudden surge in traffic or want to reduce costs during 3 periods of lower activity, AWS provides the flexibility to adjust your resources accordingly. This scalability ensures that your applications can handle varying workloads effectively.
3. Global Infrastructure: AWS has a vast global infrastructure comprising numerous data centers and availability zones spread across different regions. This infrastructure enables users to

deploy their applications and services closer to their target audience, resulting in reduced latency and improved performance.

4. Reliability and Availability: AWS has built a reputation for providing highly reliable and available services. With its multiple availability zones and data replication mechanisms, AWS ensures that your applications and data remain accessible even in the face of hardware failures or natural disasters. Service Level Agreements (SLAs) guarantee a certain level of uptime for many AWS services.
5. Security: AWS places a strong emphasis on security. It provides a wide range of security features and tools to help users protect their applications and data. This includes encryption options, network security controls, identity and access management, and compliance certifications. AWS adheres to industry best practices to maintain a secure environment for its customers.
6. Integration and Ecosystem: AWS integrates well with various third-party tools, technologies, and services. It offers extensive APIs and SDKs, making it easier to integrate AWS services into existing applications or build new solutions from scratch. The AWS ecosystem also includes a vibrant community, documentation, training resources, and support services, facilitating development and troubleshooting.
7. Cost-Effectiveness: AWS follows a pay-as-you-go pricing model, allowing users to pay only for the resources they consume. This eliminates the need for upfront investments in hardware and infrastructure. Additionally, AWS provides cost optimization tools and features to help users monitor and control their spending, ensuring cost-effectiveness.
8. Innovation and Continuous Improvement: AWS continues to innovate and expand its services, introducing new capabilities and features regularly. It invests heavily in research and development to stay at the forefront of cloud technology. This commitment to innovation ensures that users have access to the latest tools and advancements in cloud computing.

These factors, among others, contribute to the popularity and success of AWS as a cloud computing provider. However, it's important to note that the choice of cloud provider should be based on your specific needs, requirements, and preferences. It's worth evaluating multiple cloud platforms to determine the best fit for your organization.

Advantages of AWS:

1. Flexibility
2. Cost-effectiveness
3. Scalability/Elasticity
4. Security

## 1) Flexibility

- ✓ We can get more time for core business tasks due to the instant availability of new features and services in AWS.
- ✓ It provides effortless hosting of legacy applications. AWS does not require learning new technologies and migration of applications to the AWS provides advanced computing and efficient storage.
- ✓ AWS also offers a choice that whether we want to run the applications and services together or not. We can also choose to run a part of the IT infrastructure in AWS and the remaining part in data centers.

## 2) Cost-effectiveness

AWS requires no upfront investment, long-term commitment, and minimum expense when compared to traditional IT infrastructure that requires a huge investment.

## 3) Scalability/Elasticity

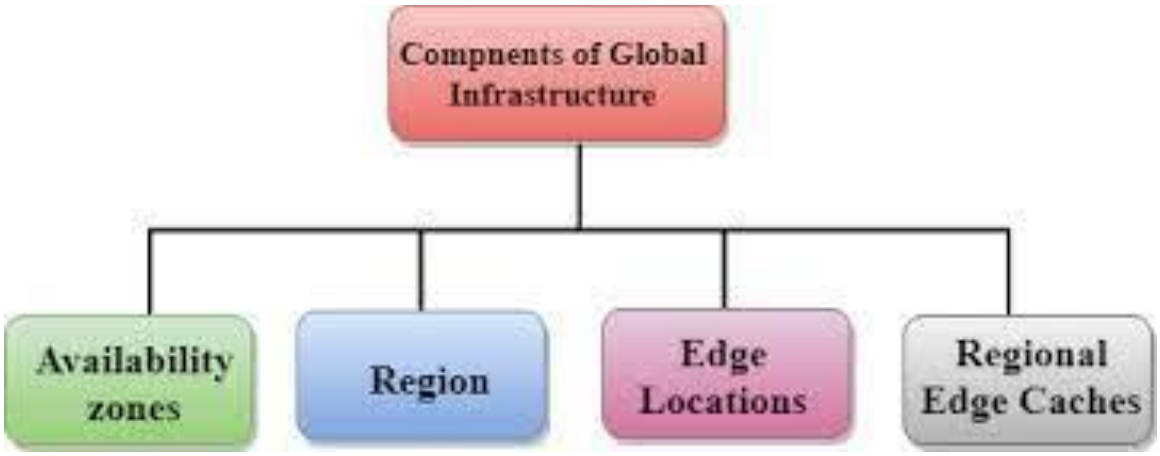
Through AWS, autoscaling and elastic load balancing techniques are automatically scaled up or down, when demand increases or decreases respectively. AWS techniques are ideal for handling 5 unpredictable or very high loads. Due to this reason, organizations enjoy the benefits of reduced cost and increased user satisfaction.

## 4) Security

- ✓ AWS is a cloud computing platform which is globally available.
- ✓ Global infrastructure is a region around the world in which AWS is based. Global infrastructure is a bunch of high-level IT services which is shown below.
- ✓ AWS is available in 19 regions, and 57 availability zones in December 2018 and 5 more regions 15 more availability zones for 2019.

The following are the components that make up the AWS infrastructure:

- ✓ Availability Zones
- ✓ Region
- ✓ Edge locations
- ✓ Regional Edge Caches




In Amazon Web Services (AWS), an Availability Zone (AZ) refers to a distinct, physically separate data center within a specific region. AZs are designed to provide fault tolerance and high availability by isolating failures and minimizing the impact of any disruption.

Each AZ is equipped with independent power, cooling, networking infrastructure, and is connected to other AZs within the same region through high-speed, low-latency links. They are strategically located to minimize the risk of natural disasters affecting multiple zones simultaneously.

By distributing resources across multiple AZs, you can design highly reliable and resilient architectures in AWS. When you launch resources like EC2 instances, databases, or storage volumes, you have the option to select the AZ in which they should be provisioned.

The primary benefits of utilizing Availability Zones in AWS include:

Fault tolerance: By deploying resources in different AZs, you protect your applications from single points of failure. If one AZ experiences an issue, your applications can continue running in other AZs, ensuring minimal downtime

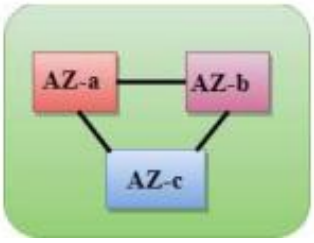
High availability: Distributing resources across AZs allows you to achieve high availability for your applications. Services like load balancers can be configured to route traffic across multiple AZs, automatically diverting traffic to healthy instances if one AZ becomes unavailable.

Availability zone as a Data Center

- ✓ An availability zone is a facility that can be somewhere in a country or in a city. Inside this facility, i.e., Data Centre, we can have multiple servers, switches, load balancing, firewalls. The things which interact with the cloud sit inside the data centers.
- ✓ An availability zone can be a several data centers, but if they are close together, they are counted as 1 availability zone.

Region

- ✓ A region is a geographical area. Each region consists of 2 more availability zones.
- ✓ A region is a collection of data centers which are completely isolated from other regions.
- ✓ A region consists of more than two availability zones connected to each other through links.




- ✓ Availability zones are connected through redundant and isolated metro fibers.

Edge Locations

- ✓ Edge locations are the endpoints for AWS used for caching content.
- ✓ Edge locations consist of CloudFront and Amazon's Content Delivery Network (CDN).
- ✓ Edge locations are more than regions. Currently, there are over 150 edge locations.
- ✓ Edge location is not a region but a small location that AWS have. It is used for caching the content.
- ✓ Edge locations are mainly located in most of the major cities to distribute the content to end users with reduced latency.
- ✓ For example, some user accesses your website from Singapore; then this request would be redirected to the edge location closest to Singapore where cached data can be read.

Regional Edge Cache

- ✓ AWS announced a new type of edge location in November 2016, known as a Regional Edge Cache.
- ✓ Regional Edge cache lies between CloudFront Origin servers and the edge locations
- ✓ A regional edge cache has a larger cache than an individual edge location.
- ✓ Data is removed from the cache at the edge location while the data is retained at the Regional Edge Caches.
- ✓ When the user requests the data, then data is no longer available at the edge location. Therefore, the edge location retrieves the cached data from the regional edge cache instead of the Origin servers that have high latency

## List of top AWS Services:

AWS is the widely used cloud platform worldwide, from start-ups to large enterprises. Though AWS services were introduced to the market by 2006, their revenue from Public Cloud SaaS has hit 145.5 billion USD by 2021. Presently, Amazon Web Services are a one-stop solution for all cloud services ranging from data storage to analytics. AWS services provide easy, simple, costeffective cloud services, which drive businesses to achieve increased efficiency and performance. Besides, these services have many more features to serve customers in multiple ways.

Now, let's have a look at the most popular AWS services in 2023. In this blog, you can learn what is the objective, features, and benefits of each AWS service.

Here is the list of Top 30 AWS Services List:

1.Amazon EC2 [Elastic Compute Cloud]

Amazon EC2 is one of the fastest-growing cloud computing AWS services, which offers virtual servers to manage any kind of workload. It facilitates the computing infrastructure with the best suitable processors, networking facilities, and storage systems. As a result, it supports adapting to the workloads precisely. Amazon EC2 provides a highly secure, reliable, performing computing infrastructure meeting business demands. And it helps you to access resources quickly and dynamically scale capacities as per demands.

2. Amazon S3

Another popular addition to the AWS services list is Amazon S3, which is an object storage AWS service, which is highly scalable. It mainly helps users to access any quantity of data from anywhere. Here, data is stored in 'storage classes' to reduce costs without any extra investment and manage it comfortably. The data is highly secure and supports meeting audit and compliance requirements. You can handle any volume of data with Amazon S3's robust access controls, replication tools, and higher visibility. Moreover, it supports maintaining data version controls and preventing accidental deletion.

3. AWS Aurora

Amazon Aurora is the next addition to this list of top AWS services in demand. Why? It is a MySQL and PostgreSQL compatible relational database with high performance. Believe it or not, it is five times faster than standard MySQL databases. And it allows for automating crucial tasks such as hardware provisioning, database setup and backups, and patching. Amazon Aurora is a distributed, fault-tolerant, self-healing storage system that could scale automatically as per needs. Besides, you can even reduce costs significantly and enhance databases' security, availability, and reliability.

4. Amazon DynamoDB

DynamoDB is a promising addition to this list of AWS services. DynamoDB is a fully managed and serverless NoSQL database AWS service. And it is a fast and flexible database system that provides innovative opportunities to developers at low costs. It gives you single-digit millisecond performance with unlimited throughput and storage. DynamoDB has in-built tools to generate actionable insights, useful analytics, and monitor traffic trends in applications.

5. Amazon RDS

Amazon RDS would be the next entry in this discussion on AWS services. Amazon RDS is the managed Relational Database AWS Service (RDS) for MySQL, PostgreSQL, Oracle, SQL Server, and MariaDB. It allows the setup, operation, and scale of a relational database in the cloud quickly. Also,

it achieves high performance by automating the tasks such as hardware provisioning, database setup, patching, and backups. When you use Amazon RDS, you don’t need to install and maintain the database software. Overall, you can optimize costs by embracing this service and achieve high availability, security, and compatibility for your resources.

6. Amazon Lambda

AWS Lambda is also a promising addition to the list of AWS services. Amazon Lambda is a serverless and event-driven computing AWS service. It helps to run codes automatically without worrying about servers and clusters. Simply put, codes can be uploaded directly to run without worrying about provisioning or managing infrastructure. So, this service automatically accepts 'code execution requests' irrespective of its scale. Besides, you can pay the price only for the computer time, so AWS Lambda makes effective cost-control.

7. Amazon VPC

Amazon VPC is the Virtual Private Cloud, which is an isolated cloud resource. It controls the virtual networking environment, such as resource placement, connectivity, and security. And it allows you to build and manage compatible VPC networks across cloud AWS resources and onpremise resources. Here, it improves security by applying rules for inbound and outbound connections. Also, it monitors VPC flow logs delivered to Amazon S3 and Amazon Cloudwatch to gain visibility over network dependencies and traffic patterns. Amazon VPC also detects anomalies in the patterns, prevents data leakage, and troubleshoots network connectivity and configuration issues.

8. Amazon CloudFront

Amazon CloudFront is another credible mention in the list of renowned Amazon Web Services. This AWS service delivers content globally, which offers high performance and security. Mainly, it delivers data with high speed and low latency. Here, content is delivered to destinations successfully with automated network mapping and intelligent routing mechanisms. The security of data is enhanced

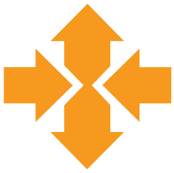
with traffic encryption methods and access controls. Also, data can be transferred within milliseconds with its in-built data compression, edge computing capabilities, and field-level encryption. Besides, you gear up streaming high-quality video using AWS media services to any device quickly and consistently using Amazon CloudFront.


9. AWS Elastic Beanstalk

This AWS service supports running and managing web applications. Elastic Beanstalk allows for the easy deployment of applications from capacity provisioning, load balancing, and autoscaling to application health monitoring. With its auto-scaling properties, this service simplifies demands in scaling to adjust to the needs of the business. It helps to manage peaks in workloads and traffic with minimum costs. Basically, AWS Elastic Beanstalk is a developer-friendly tool since it manages servers, load balancers, firewalls, and networks simply. As a result, this service allows developers to show much more focus on coding.

10. Amazon EC2 Auto-scaling

This AWS service scales computing capacity to meet the demands accurately. And it is achieved by adding or removing EC2 instances automatically. There are two types of scaling such as dynamic scaling and predictive scaling. Here, dynamic scaling responds to the presently changing demands, whereas predictive scaling responds based on predictions. Through Amazon EC2 Auto-scaling, you can identify the unhealthy EC2 instances, terminate them, and replace them with new instances.



11. Amazon ElastiCache

Amazon ElastiCache is a fully managed, flexible, in-memory caching AWS service. It supports increasing the performance of your applications and database. And this service helps to reduce the load in a database by caching data in memory. Amazon ElastiCache accesses data from inmemory with high speed, microsecond latency, and high throughput. With a self-managed cache service, you can reduce costs and eliminate the operational overhead of your business.

12. Amazon S3 Glacier

Amazon S3 Glacier is the archive storage in the cloud at a low cost. It is built with three storage classes such as S3 Glacier instant retrieval, flexible retrieval, and deep archive. Here, the instant class supports immediate access to data, and the flexible class allows flexible access within minutes to hours with no cost. The third one, deep archive, helps archive compliance data and digital media. Overall, they support you to access data from archives faster.

13. Amazon LightSail

Amazon LightSail is the website and applications building AWS service. This service offers Virtual Private Server instances, containers, databases, and storage. It allows a serverless computing service with AWS Lambda. With Amazon LightSail, you can create websites using pre-configured applications such as WordPress, Magento, Prestashop, and Joomla in a few clicks and at a low cost. In addition to this, it is the best tool for testing, so you can create, test, and delete sandboxes with your new ideas.

14. Amazon Sagemaker

Amazon Sagemaker is the AWS service that allows building, training, and deploying Machine Learning (ML) models at a large capacity. It is an analytical tool that functions based on Machine Learning power to analyze data more efficiently. With its single toolset, you can build high-quality ML models quickly. Amazon Sagemaker not only generates reports but provides the purpose for generating predictions too. In addition, Amazon Ground Truth Plus creates datasets without labeling applications.

15. Amazon SNS

It is the Amazon Simple Notification Service (SNS). It is a messaging service between Application to Application (A2P) and Application to Person (A2Person). Here, A2P helps many-to-many messaging between distributed systems, microservices, and event-driven serverless applications. And A2P supports applications to send messages to many users via mail, SMS, etc. For instance, you can send up to ten messages in a single API request. With effective filtering systems, subscribers will receive messages that they are interested in. Besides, Amazon SNS works alongside Amazon SQS to deliver messages accurately and consistently

16. Amazon EBS

Amazon Elastic Block Store (EBS) is a block storage service. It supports scaling highperformance workloads such as SAP, Oracle, and Microsoft products. And it provides better 14 protection against failures up to 99.999%. It helps to resize clusters for big data analytics engines such as Hadoop and Spark. Also, you can build storage volumes, optimize storage performance, and reduce costs. Amazon EBS's lifecycle management creates policies that help create and manage backups effectively.

17. Amazon Kinesis

It is the AWS service that analyses video as well as data streams. Amazon Kinesis collects, processes, and analyzes all types of streaming data. Here, the data may be audio, video, application logs, website clickstreams, and IoT telemetry. Then, it generates real-time insights within seconds once the data has arrived. With the help of Amazon Kinesis, you could stream and process a large quantity of real-time data with low latencies, very simply.

18. Amazon Elastic File System (EFS)

Amazon EFS is the fully managed file system for Amazon EC2. And it is a simple and serverless elastic file system. You can create and configure file systems without provisioning, deploying, patching, and

maintenance using Amazon EFS. Here, files can be added and deleted as per the scaling needs. Especially, you can pay only for the used space, hence this service helps to reduce costs.

19. AWS IAM

It is the Identity and Access Management (IAM) service offered by AWS to securely access the applications and resources. It regulates access to various resources based on roles and access policies; as a result, you can achieve a fine-grained access control on your resources. The AWS IAM access analyzer helps streamline permission management through setting, verifying, and refining. In addition, AWS IAM attribute-based access control helps create fine-grained permissions based on user attributes such as department, job role, team name, etc.

20. Amazon SQS

Amazon SQS is a fully managed message queuing service. There are two types of message queuing services: SQS Standard and SQS FIFO. Here, the SQS standard offers features such as maximum throughput, best-effort ordering, and quick delivery. And SQS FIFO processes messages only once in the same order by which they have been sent. Also, Amazon SQS allows decoupling or scaling microservices, distributed systems, and serverless applications. It helps you send, receive, and manage messages in a large volume. Moreover, there is no need to install and maintain other messaging software, reducing costs significantly. Besides, scaling is carried out quickly and automatically in this service.

21. Amazon RedShift

Amazon Redshift is a quick, simple, and cost-effective data warehousing service. You can gain insights about cloud data warehousing in an easy, faster, and more secure way. It allows analysis of all the

data in operational databases, data lakes, data warehouses, and third-party data. And Amazon Redshift helps analyze a large volume of data and run complex analytical queries. With its automation capabilities, this service increases query speed and provides the best price performance.

22. Amazon Cloudwatch

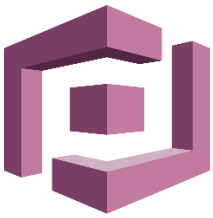
This AWS service monitors the cloud resources and applications keenly. It is a single platform that helps to monitor all AWS resources and applications; it increases visibility to respond to issues quickly. Mainly, Amazon Cloudwatch provides actionable insights to optimize monitoring applications, systemwide performance changes, and resource utilization. And you can get a complete view of the health of AWS resources, applications, and services running on AWS and on-premises. In addition, Amazon CloudWatch helps to detect anomalies in the behavior of the cloud environment, set alarms, visualize logs and metrics, make automated actions, troubleshoot issues, and discover insights

23. Amazon Chime

Amazon Chime is a communication service. It is a single solution that offers audio calling, video calling, and screen sharing capabilities. With the help of this service, you can make quality meetings, chat, and video calls both inside and outside of your organization. And more features can be added to this service as per your business needs. Mainly, you can set calls for a predefined time to automatically make calls on time. Amazon Chime helps you not to miss a meeting amidst your hectic schedule at work. Besides, you can pay as per the usage of resources by which you can reduce the costs significantly.

24. Amazon Cognito

It is the identity management AWS service. Amazon Cognito manages identities for accessing your applications and resources. Mainly, this service helps to add sign-in, sign-up, and access control the web and mobile apps quickly. It can support millions of users to sign in with familiar applications such as Apple, Facebook, Google, and Amazon. In Amazon Cognito, the feature 'Cognito user pools' can be set up quickly without any infrastructure, and the pool members will have a directory profile. It supports multi-factor authentication and encryption of data-at-rest and data-in-transit



25. Amazon Inspector

Amazon Inspector is an automated vulnerability management service. This service offers continuous and automated vulnerability management for Amazon EC2 and Amazon ECR. It allows scanning AWS workloads for software vulnerabilities and unwanted network exposure. Amazon Inspector quickly identifies vulnerabilities, which helps to take immediate actions to resolve them before it worsens the applications. Moreover, it supports meeting compliance requirements and reduces meantime-to-remediate vulnerabilities. And it provides you with accurate risk scores and streamlined workflow.

26. AWS Firewall Manager

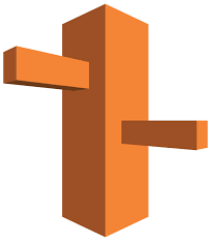
It is the central management service of firewall rules. The firewall manager supports managing firewall rules across all the applications and accounts. The common security rules help to manage new applications included over time. It is the one-time solution for consistently creating firewall rules and security policies and implementing them across the infrastructure. AWS firewall manager helps you audit VPC security groups for compliance requirements and control network traffic effectively.

27. Amazon Appflow

Amazon Appflow is a no-code service that allows the integration of SaaS applications and AWS services effortlessly. To be more precise, it securely automates dataflows integrating third-party applications and AWS services without using codes. You can transfer data between SaaS applications such as Salesforce, SAP, Zendesk, etc. since 18 Amazon Appflow can be integrated with other applications in a few clicks. Especially, a large volume of data can be moved without breaking it up into batches using this service.


28. Amazon Route 53

It is a scalable cloud Domain Name System (DNS) service. It allows end-users to connect with Amazon EC2, Elastic load balancers, Amazon S3 buckets, and even outside AWS. In this service, the feature 'Route 53 application recovery controllers' configure DNS health checks and helps to monitor the ability of systems to recover from failures. And 'Route 53 traffic flow' helps manage traffic across the globe using routing methods such as latency-based routing, Geo DNS, Geoproximity, and weighted round-robin



29. AWS Cloud Formation

This AWS service creates and manages resources with templates. It is a single platform that can handle all AWS accounts across the globe. It automates resource management with AWS service integration and offers turnkey application distribution and governance controls. Also, AWS Cloud Formation can automate, test, and deploy infrastructure with continuous integration and delivery. And you can run applications right from AWS EC2 to complex multi-region applications using this Service.

30. AWS Key Management Service (KMS)

AWS KMS manages the creation and control of encryption keys. It means that AWS KMS creates cryptographic keys and controls their uses across various applications. You can achieve a secure and resilient service using hardware resilient modules to protect keys. This service can be integrated with AWS Cloudtrail to provide logs of all key usage to precisely fulfil compliance and regulatory requirements.

# Implementation of the Architecture of Aws-Vpc-Subnetting-Auditing-Monitoring

## Introduction:

In the modern era of cloud computing, the ability to build scalable and secure infrastructures is of paramount importance. Amazon Web Services (AWS) has emerged as a leading cloud service provider, offering a wide array of tools and services to construct robust architectures. This project report outlines the creation of an architectural infrastructure utilizing AWS Virtual Private Cloud (VPC) with 20 subnets, incorporating auditing through CloudTrail logs, and implementing monitoring capabilities with CloudWatch.

## 1. Overview of AWS VPC:

The AWS Virtual Private Cloud (VPC) provides a private, isolated network environment within the AWS cloud. This project focuses on the creation of a custom VPC, which enables us to have complete control over network configuration, including IP address ranges, subnets, and routing tables. By designing a VPC, we can securely host our resources while ensuring seamless communication between them.

## 2. Subnet Configuration:

A crucial aspect of our architectural infrastructure lies in subdividing the VPC into smaller, manageable units known as subnets. We will create 20 subnets within the VPC, strategically distributed across different availability zones (AZs) to achieve high availability and fault tolerance. This segmentation ensures that resources are efficiently allocated and isolated, optimizing network performance and security.

## 3. Auditing with CloudTrail:

AWS CloudTrail offers an essential auditing mechanism that tracks and records all activities and events within our AWS environment. By enabling CloudTrail, we can gain valuable insights into resource usage, API calls, and user activity, facilitating the identification of potential security risks and aiding in compliance auditing. This project will implement CloudTrail to enhance the overall security posture of our infrastructure.

## 4. Monitoring with CloudWatch:

To maintain a proactive and vigilant approach to infrastructure management, we will incorporate AWS CloudWatch. CloudWatch provides real-time monitoring and alerts, enabling us to track metrics, set up alarms, and respond swiftly to any issues or anomalies that may arise. By leveraging

CloudWatch, we can ensure optimal performance, resource utilization, and cost-effectiveness of our AWS services.

**5. Benefits and Outcomes:**

Throughout this project, we will explore the benefits and outcomes of utilizing AWS services to build our architectural infrastructure. These include enhanced security, scalability, fault tolerance, efficient resource allocation, and improved visibility into our AWS environment. Additionally, we will analyze the impact of CloudTrail and CloudWatch on mitigating potential risks and optimizing overall operational efficiency.

## Services used :

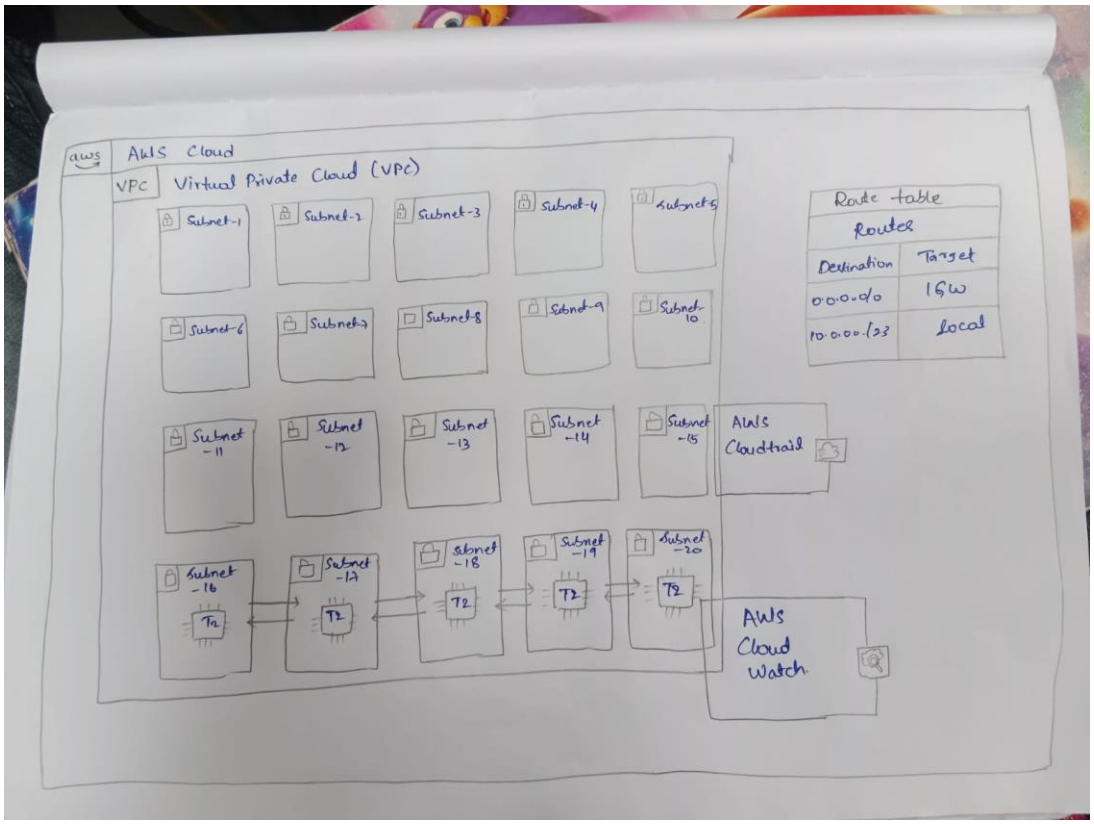
a.Virtual Private Cloud

b.Elastic Compute Cloud

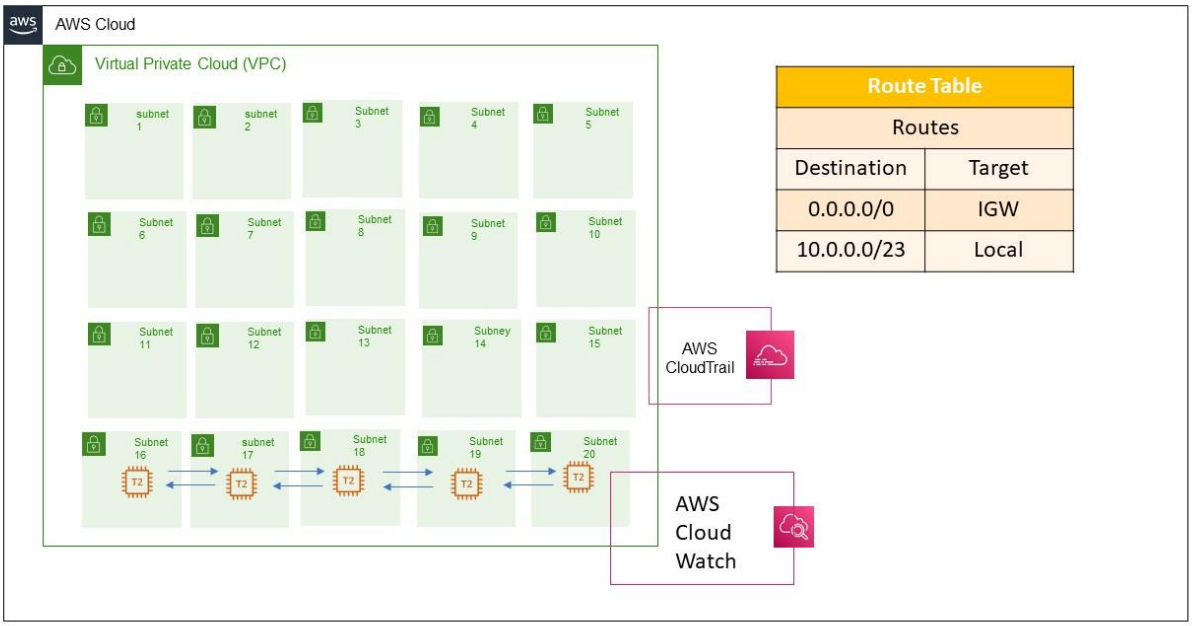
c. Cloud Log Trail

d .CloudWatch

## Rough Architect :



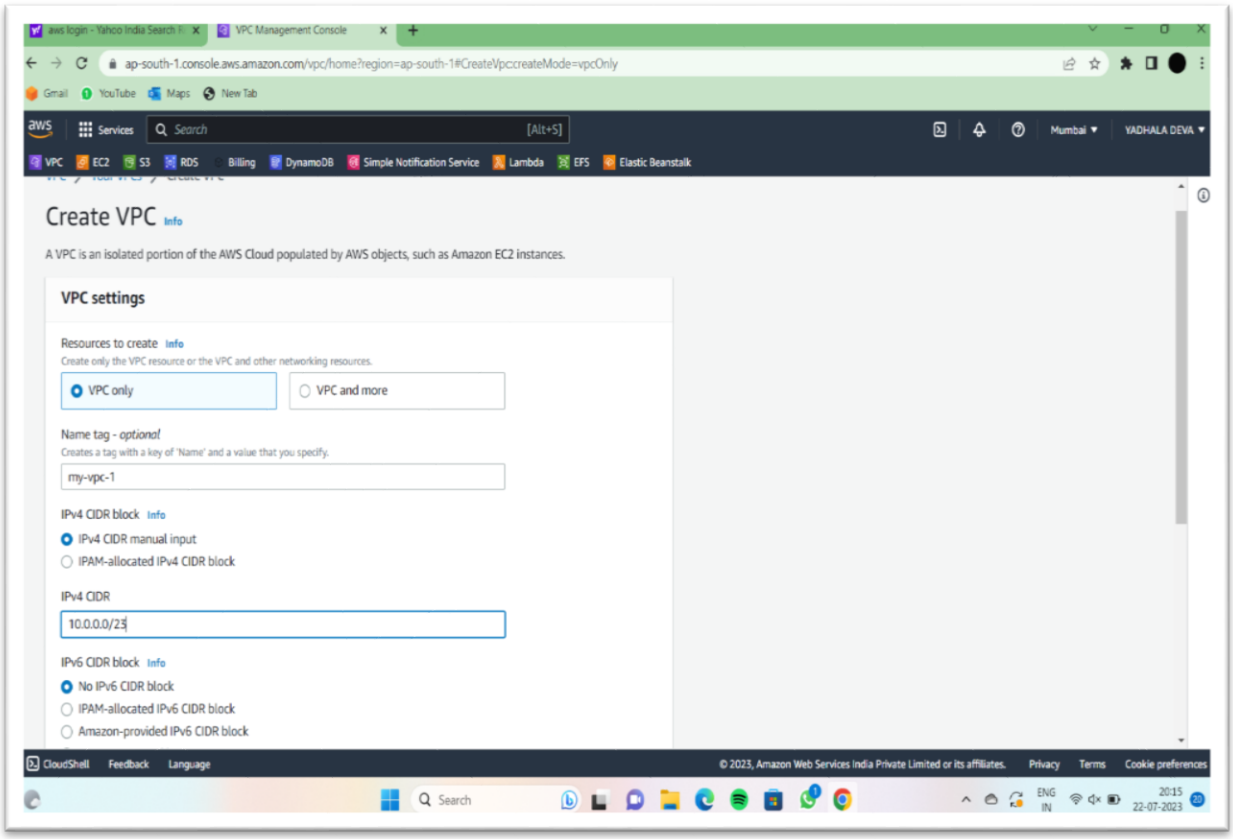
## Final Architect:

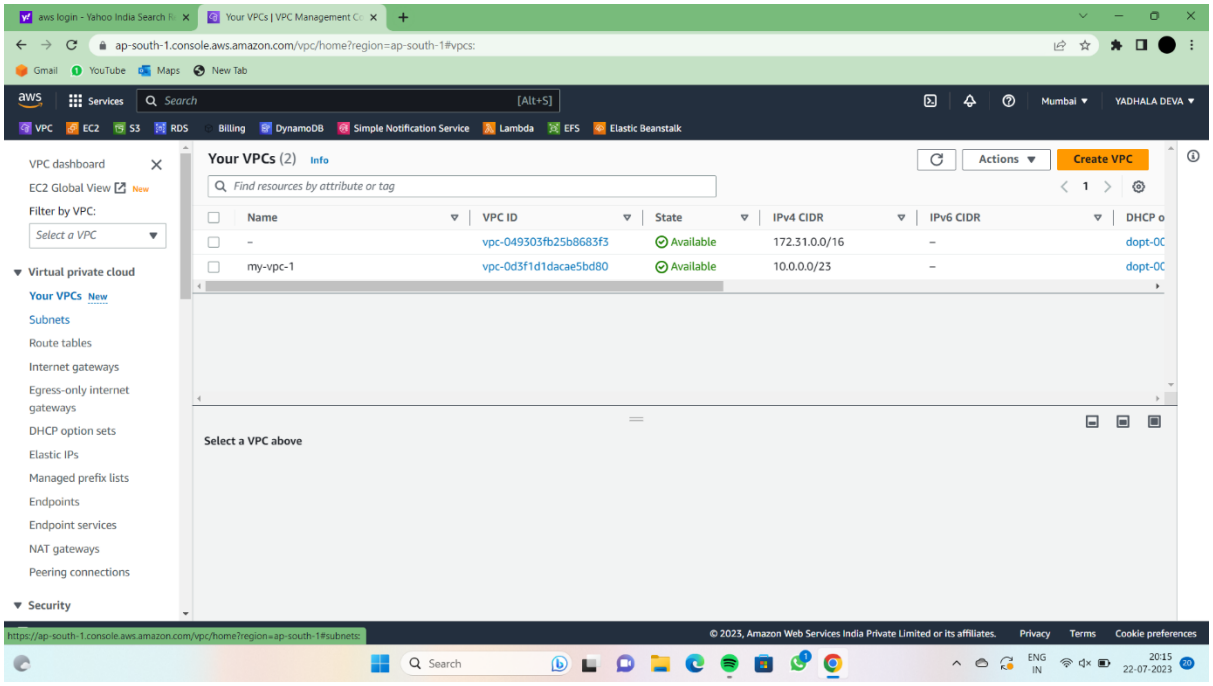


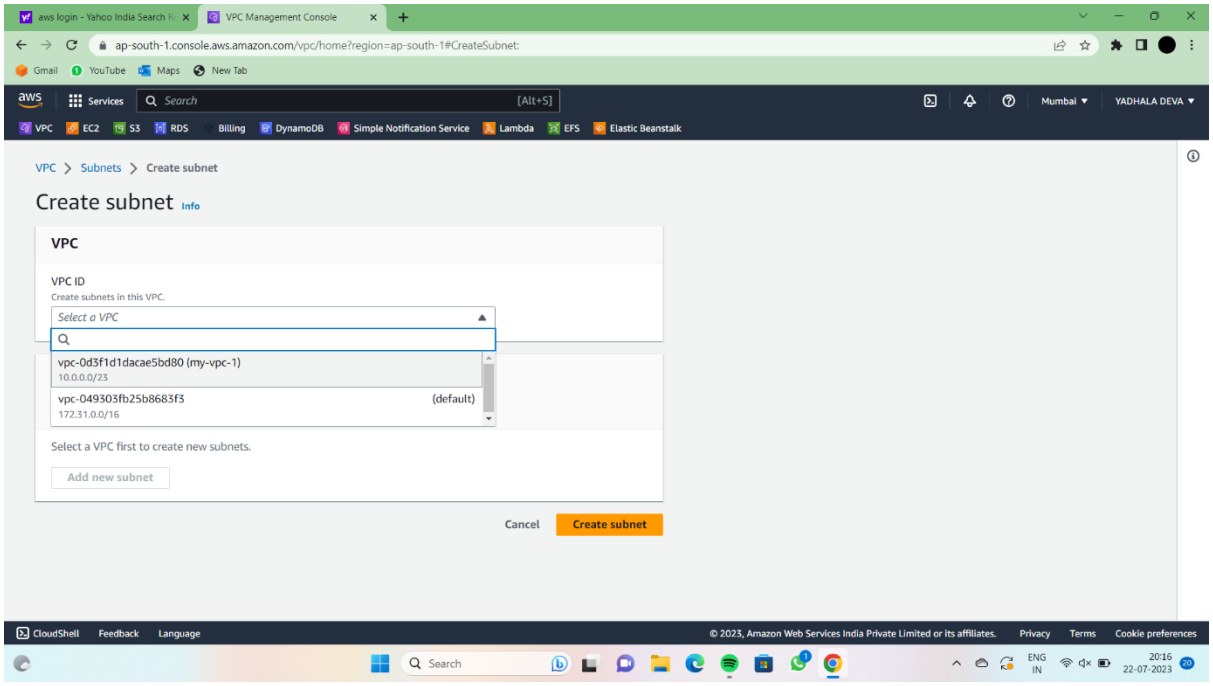

**Implementation of the Project:**

**Service 1:** VPC

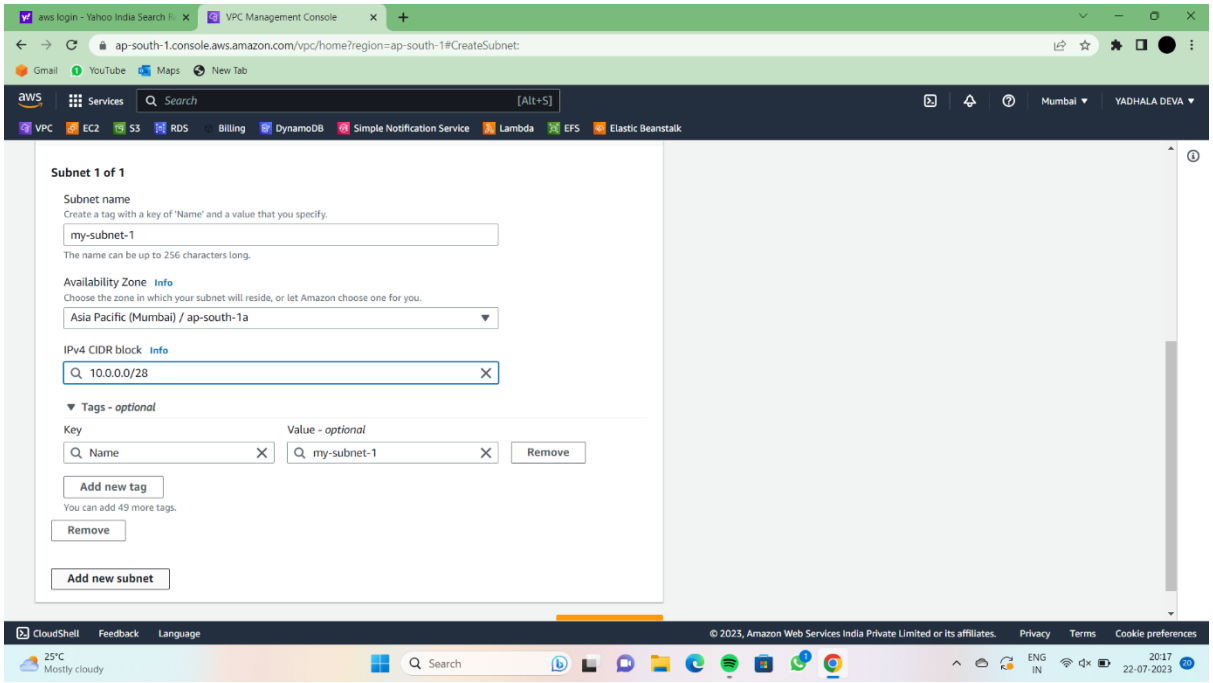
- Sign in to AWS Management Console.
- Navigate to the VPC service.
- Click "Create VPC."
- Configure VPC settings (Name, IPv4 CIDR block).
- (Optional) Configure IPv6, Tenancy, and Advanced options.
- (Optional) Add tags for better organization.
- Click "Create VPC."

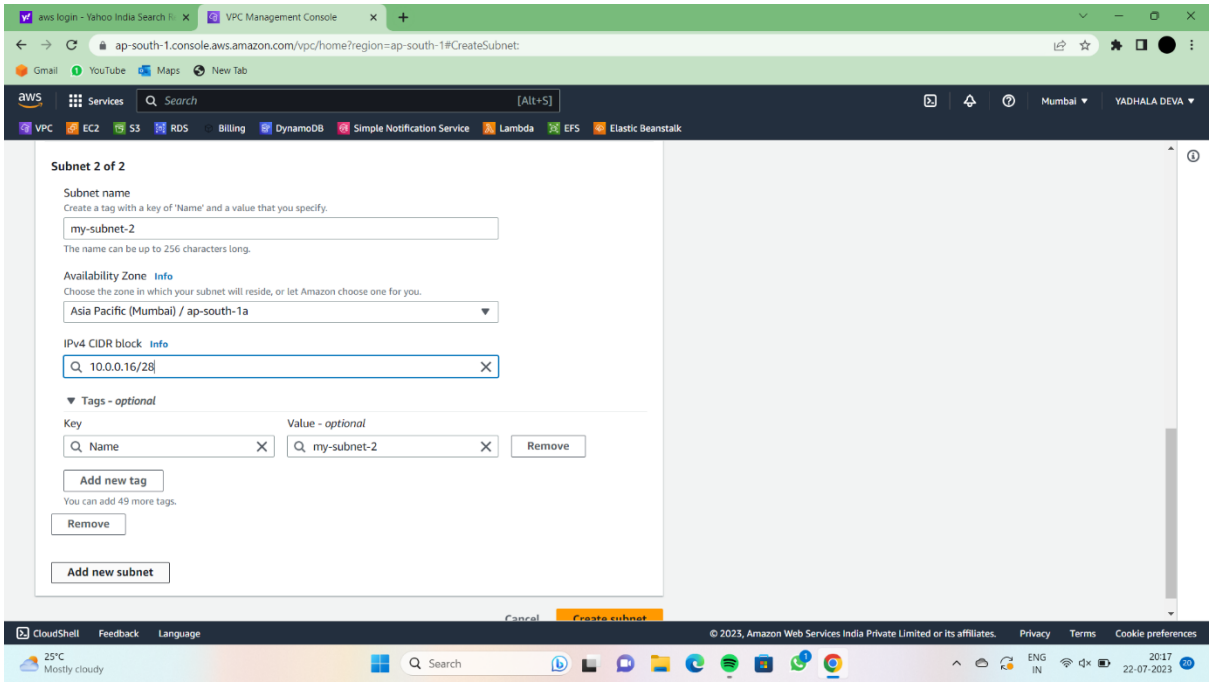

Create VPC Info
A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.
VPC settings
Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
VPC only
VPC and more
Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.
my-vpc-1
IPv4 CIDR block Info
IPv4 CIDR manual input
IPAM-allocated IPv4 CIDR block
IPv4 CIDR
10.0.0.0/23
IPv6 CIDR block Info
No IPv6 CIDR block
IPAM-allocated IPv6 CIDR block
Amazon-provided IPv6 CIDR block


Your VPCs (2) Info
Actions
Create VPC
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
vpc-049303fb25b8683f3
Available
172.31.0.0/16
my-vpc-1
vpc-0d3f1d1dacae5bd80
Available
10.0.0.0/23
Select a VPC above

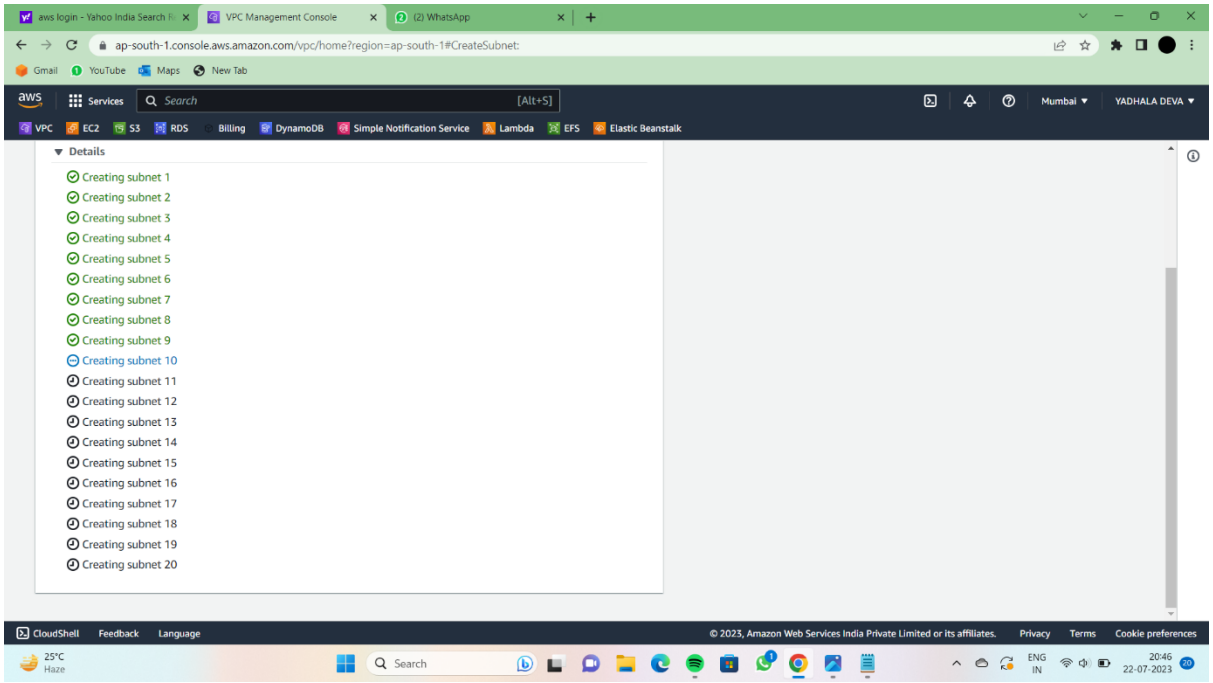



- Select a vpc id of vpc1.
- Then,click on add new subnet.
- Give availability zone ap-south-1a and CIDR-10.0.0.0/28.



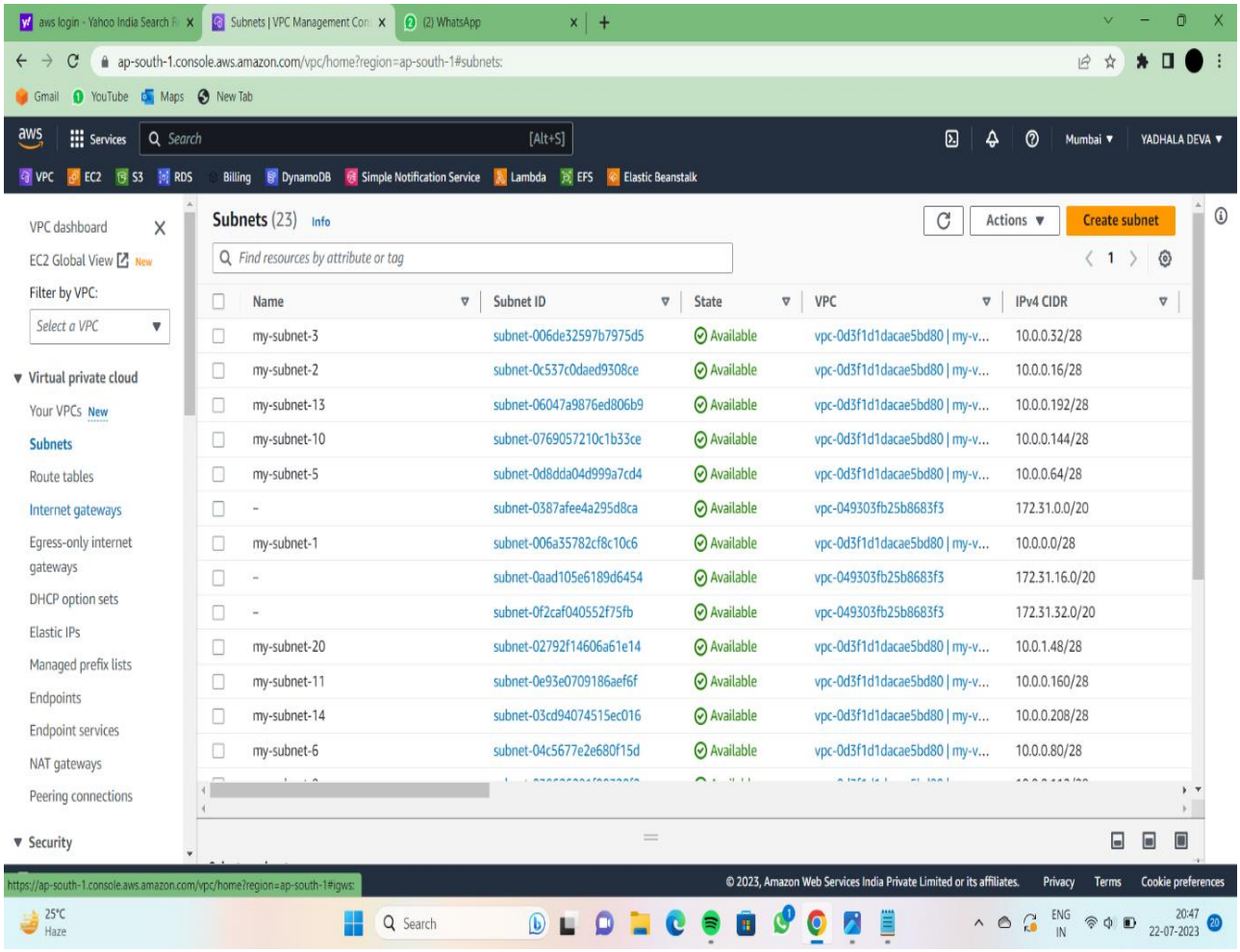



- Likewise we need to create 20 subnets with same region and different CIDR addresses in same vpc.
- After that click on create subnet.

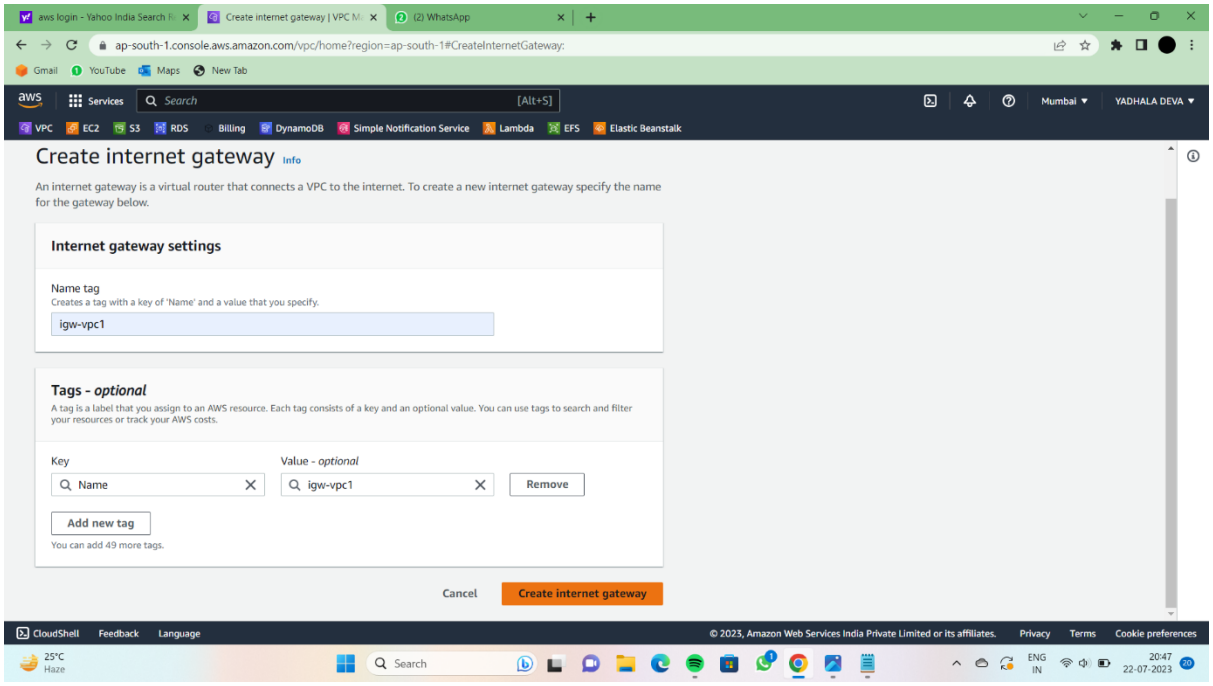


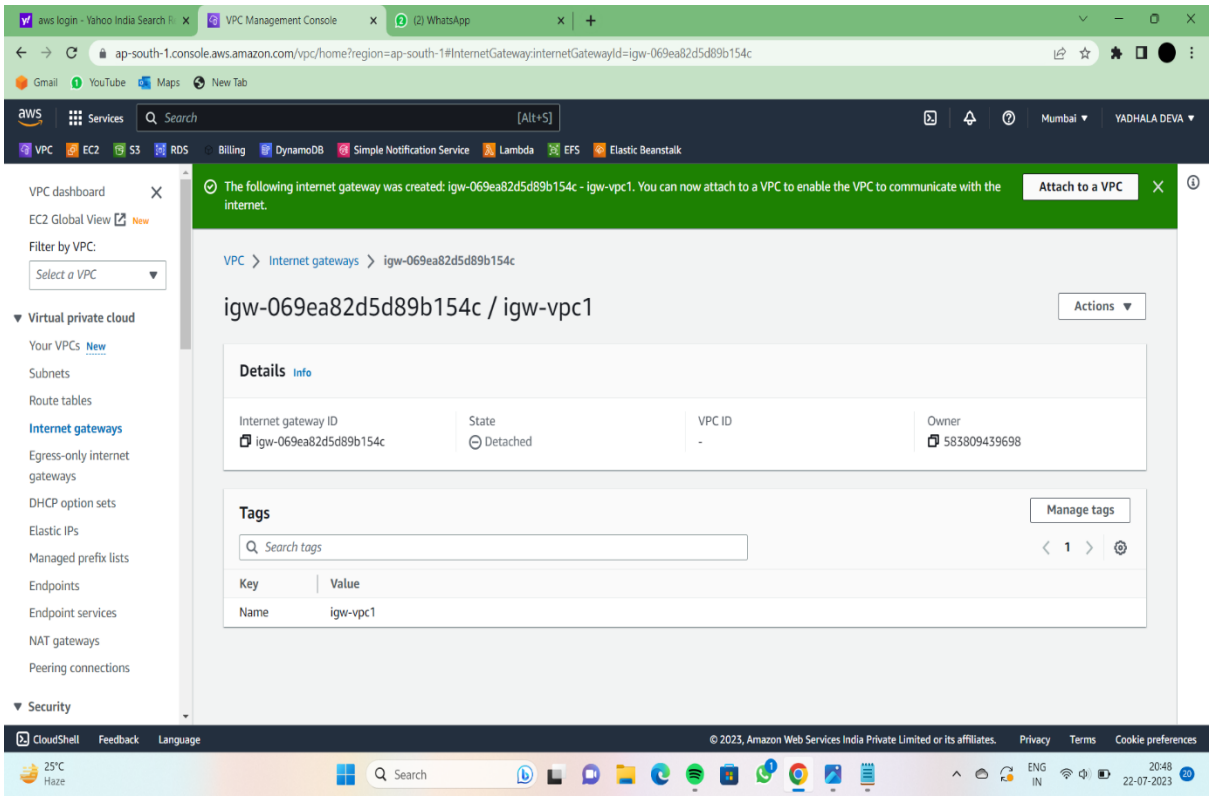

- Creation of subnets are running.

- The 20subnets are created

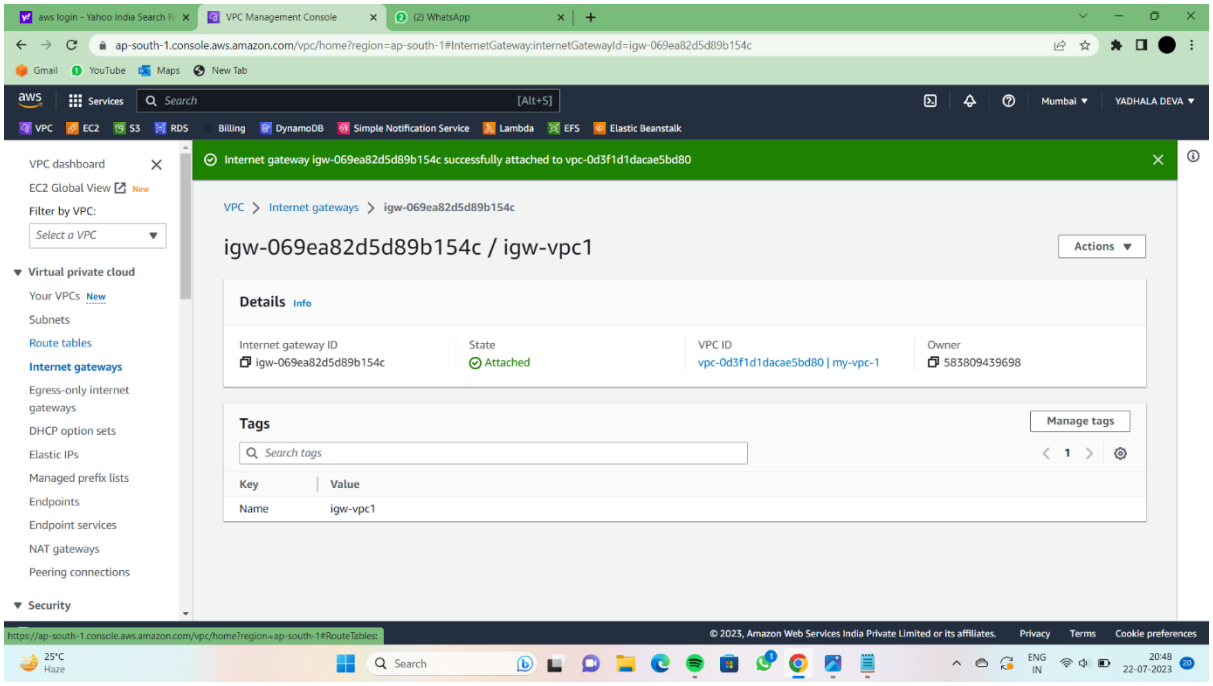



- Go to intenet gateway and click on create internet gateway.
- Give name tag=igw-vpc1
- And click on create internet gateway.

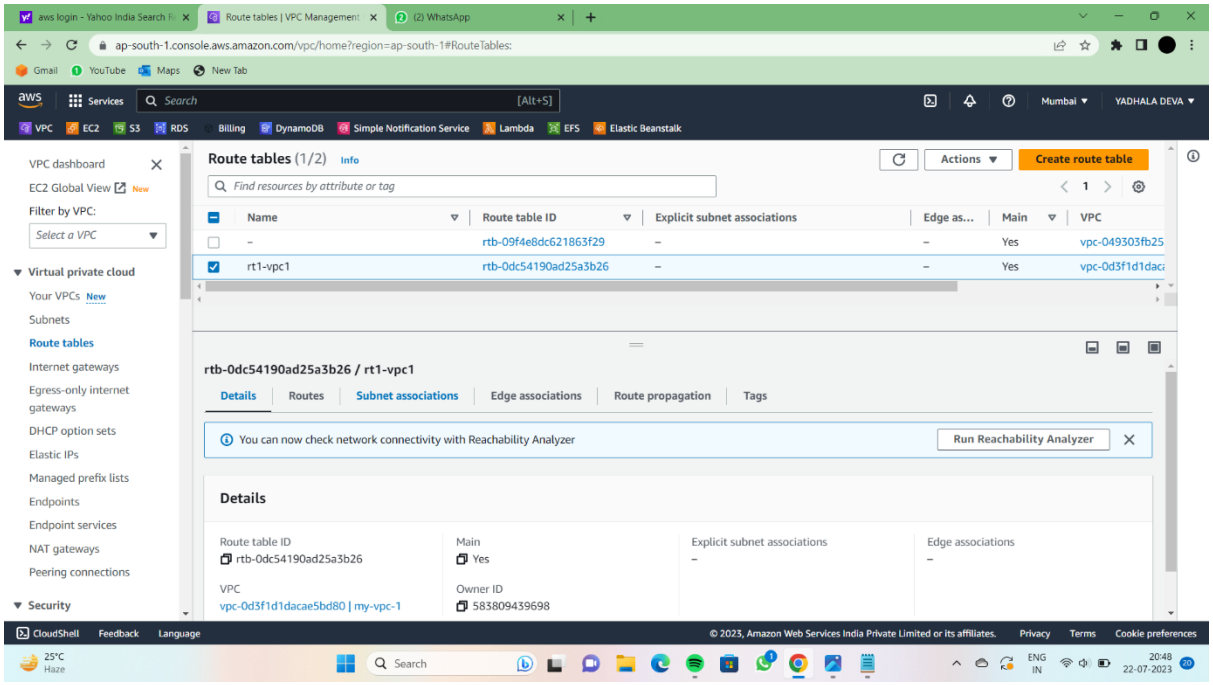


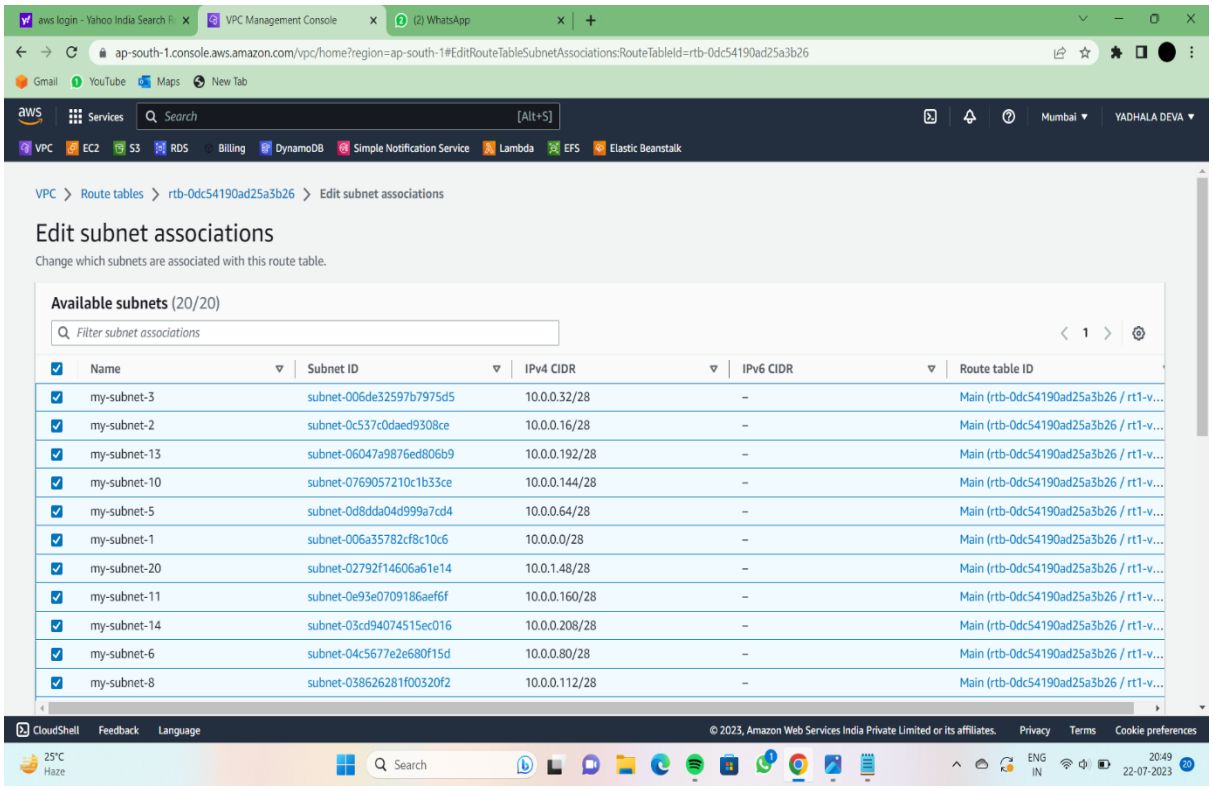

- After creation of internet gateway, click on attach to a VPC.
- Then,Give VPC1 id and click on attach internet gateway.

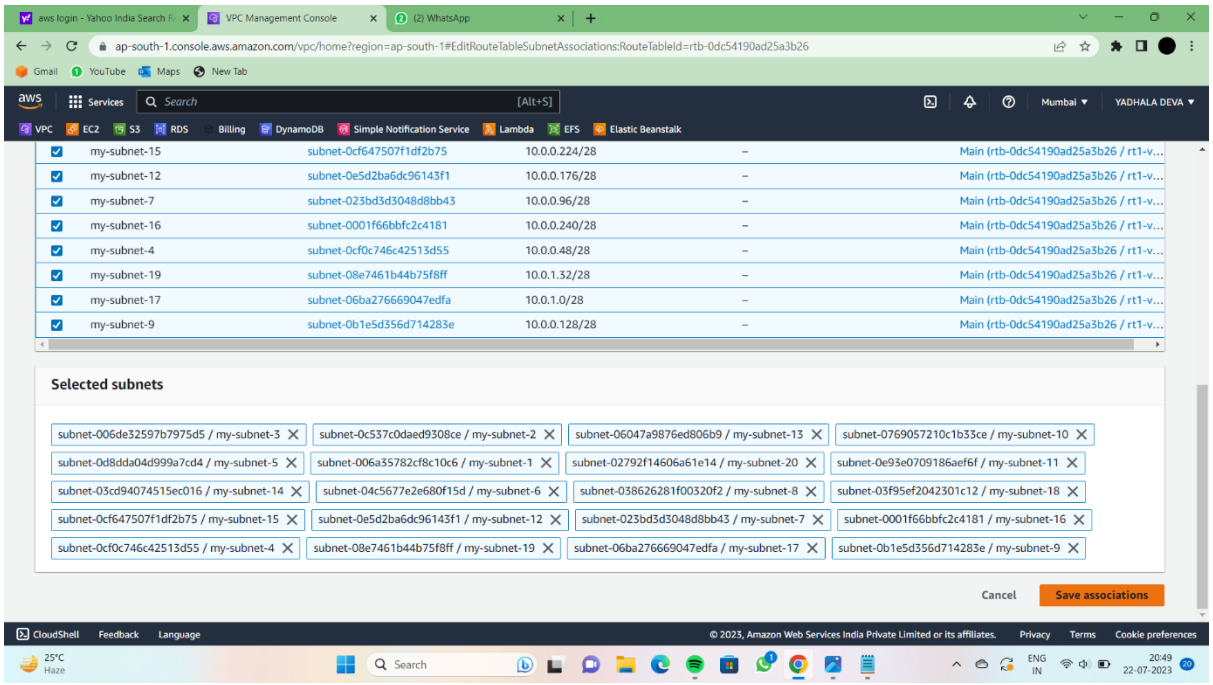


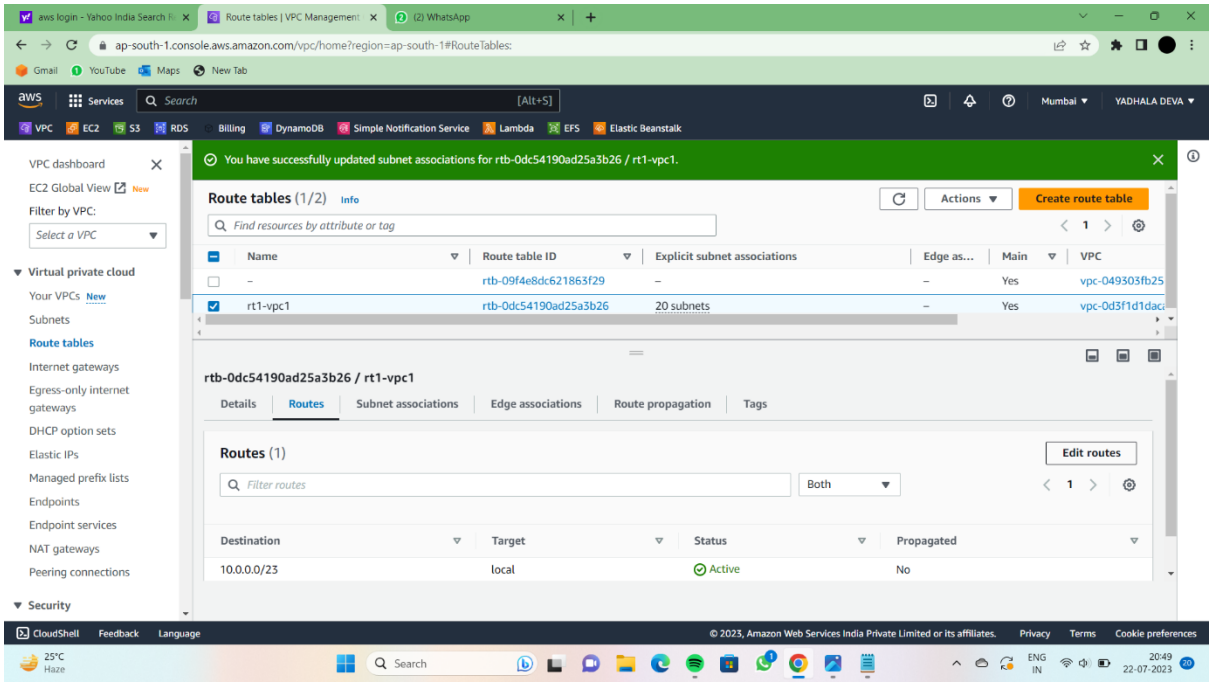

- Go to route tables and edit the name of the route table as rt1-vpc1 that is created along with vpc1.



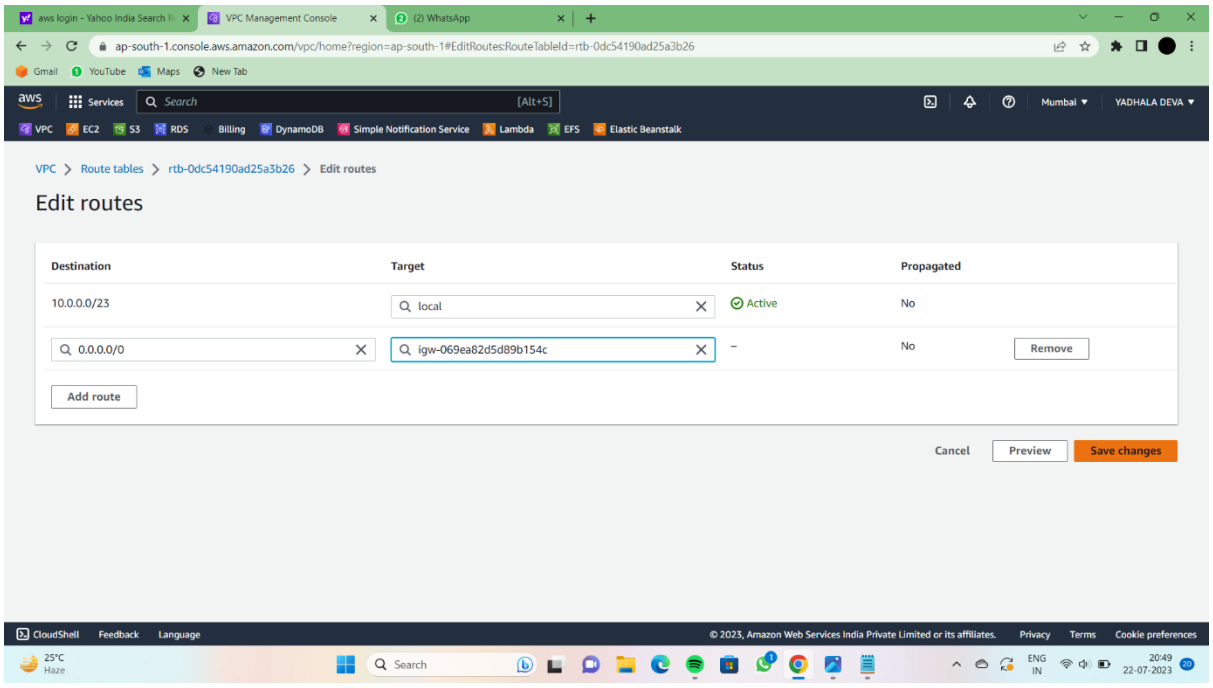

- Go to route tables,select the public route table, and go to subnet associations and select public subnets and click on save associations.


aws login - Yahoo India Search R
VPC Management Console
(2) WhatsApp
ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#EditRouteTableSubnetAssociations:RouteTableId=rtb-0dc54190ad25a3b26
Gmail
YouTube
Maps
New Tab
Services
Search
[Alt+S]
Mumbai
YADHALA DEVA
VPC
EC2
S3
RDS
Billing
DynamoDB
Simple Notification Service
Lambda
EFS
Elastic Beanstalk
VPC > Route tables > rtb-0dc54190ad25a3b26 > Edit subnet associations
Edit subnet associations
Change which subnets are associated with this route table.
Available subnets (20/20)
Filter subnet associations
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
Route table ID
my-subnet-3 subnet-006de32597b7975d5 10.0.0.32/28 – Main (rtb-0dc54190ad25a3b26 / rt1-v...
my-subnet-2 subnet-0c537c0daed9308ce 10.0.0.16/28 – Main (rtb-0dc54190ad25a3b26 / rt1-v...
my-subnet-13 subnet-06047a9876ed806b9 10.0.0.192/28 – Main (rtb-0dc54190ad25a3b26 / rt1-v...
my-subnet-10 subnet-0769057210c1b33ce 10.0.0.144/28 – Main (rtb-0dc54190ad25a3b26 / rt1-v...
my-subnet-5 subnet-0d8dda04d999a7cd4 10.0.0.64/28 – Main (rtb-0dc54190ad25a3b26 / rt1-v...
my-subnet-1 subnet-006a35782cf8c10c6 10.0.0.0/28 – Main (rtb-0dc54190ad25a3b26 / rt1-v...
my-subnet-20 subnet-02792f14606a61e14 10.0.1.48/28 – Main (rtb-0dc54190ad25a3b26 / rt1-v...
my-subnet-11 subnet-0e93e0709186aef6f 10.0.0.160/28 – Main (rtb-0dc54190ad25a3b26 / rt1-v...
my-subnet-14 subnet-03cd94074515ec016 10.0.0.208/28 – Main (rtb-0dc54190ad25a3b26 / rt1-v...
my-subnet-6 subnet-04c5677e2e680f15d 10.0.0.80/28 – Main (rtb-0dc54190ad25a3b26 / rt1-v...
my-subnet-8 subnet-038626281f00320f2 10.0.0.112/28 – Main (rtb-0dc54190ad25a3b26 / rt1-v...
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
25°C
Haze
Search
ENG
IN
20:49
22-07-2023


aws login - Yahoo India Search R
VPC Management Console
(2) WhatsApp
ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#EditRouteTableSubnetAssociations:RouteTableId=rtb-0dc54190ad25a3b26
Gmail
YouTube
Maps
New Tab
Services
Search
[Alt+S]
Mumbai
YADHALA DEVA
VPC
EC2
S3
RDS
Billing
DynamoDB
Simple Notification Service
Lambda
EFS
Elastic Beanstalk
my-subnet-15 subnet-0cf647507f1df2b75 10.0.0.224/28 – Main (rtb-0dc54190ad25a3b26 / rt1-v...
my-subnet-12 subnet-0e5d2ba6dc96143f1 10.0.0.176/28 – Main (rtb-0dc54190ad25a3b26 / rt1-v...
my-subnet-7 subnet-023bd3d3048d8bb43 10.0.0.96/28 – Main (rtb-0dc54190ad25a3b26 / rt1-v...
my-subnet-16 subnet-0001f66bbfc2c4181 10.0.0.240/28 – Main (rtb-0dc54190ad25a3b26 / rt1-v...
my-subnet-4 subnet-0cf0c746c42513d55 10.0.0.48/28 – Main (rtb-0dc54190ad25a3b26 / rt1-v...
my-subnet-19 subnet-08e7461b44b75f8ff 10.0.1.32/28 – Main (rtb-0dc54190ad25a3b26 / rt1-v...
my-subnet-17 subnet-06ba276669047edfa 10.0.1.0/28 – Main (rtb-0dc54190ad25a3b26 / rt1-v...
my-subnet-9 subnet-0b1e5d356d714283e 10.0.0.128/28 – Main (rtb-0dc54190ad25a3b26 / rt1-v...
Selected subnets
subnet-006de32597b7975d5 / my-subnet-3
subnet-0c537c0daed9308ce / my-subnet-2
subnet-06047a9876ed806b9 / my-subnet-13
subnet-0769057210c1b33ce / my-subnet-10
subnet-0d8dda04d999a7cd4 / my-subnet-5
subnet-006a35782cf8c10c6 / my-subnet-1
subnet-02792f14606a61e14 / my-subnet-20
subnet-0e93e0709186aef6f / my-subnet-11
subnet-03cd94074515ec016 / my-subnet-14
subnet-04c5677e2e680f15d / my-subnet-6
subnet-038626281f00320f2 / my-subnet-8
subnet-03f95ef2042301c12 / my-subnet-18
subnet-0cf647507f1df2b75 / my-subnet-15
subnet-0e5d2ba6dc96143f1 / my-subnet-12
subnet-023bd3d3048d8bb43 / my-subnet-7
subnet-0001f66bbfc2c4181 / my-subnet-16
subnet-0cf0c746c42513d55 / my-subnet-4
subnet-08e7461b44b75f8ff / my-subnet-19
subnet-06ba276669047edfa / my-subnet-17
subnet-0b1e5d356d714283e / my-subnet-9
Cancel
Save associations
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
25°C
Haze
Search
ENG
IN
20:49
22-07-2023

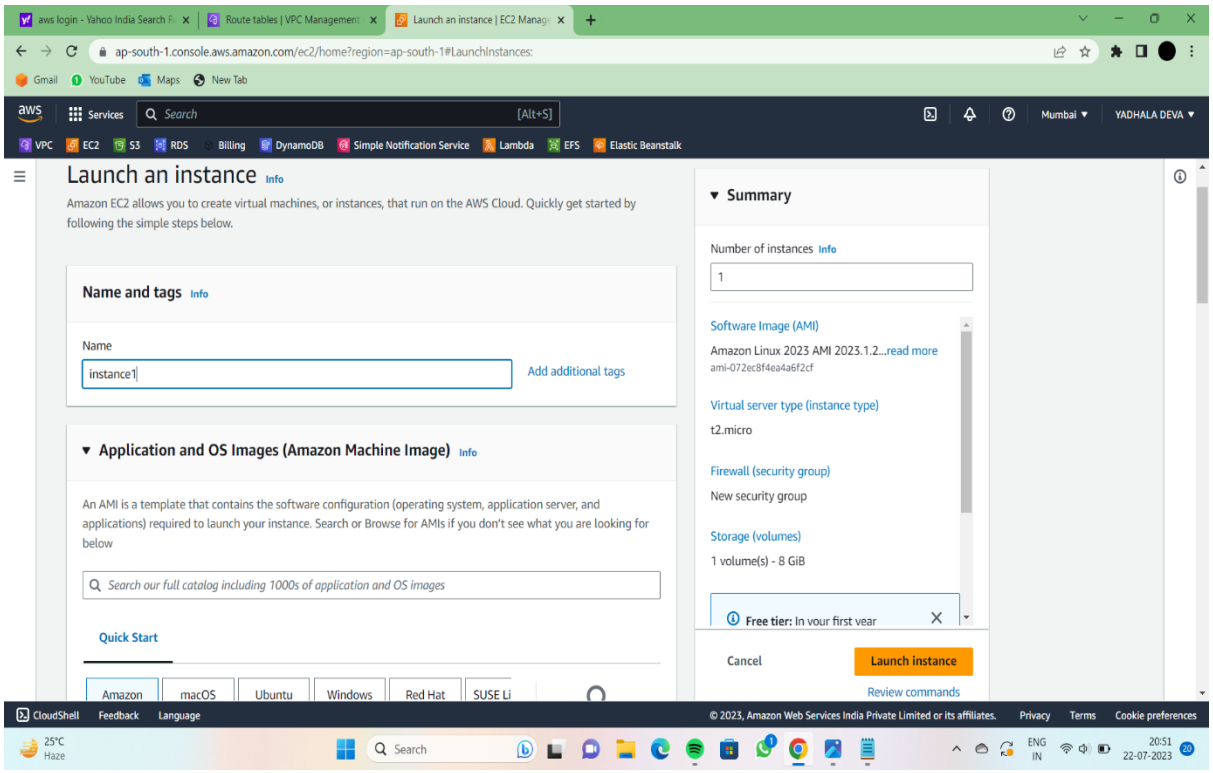


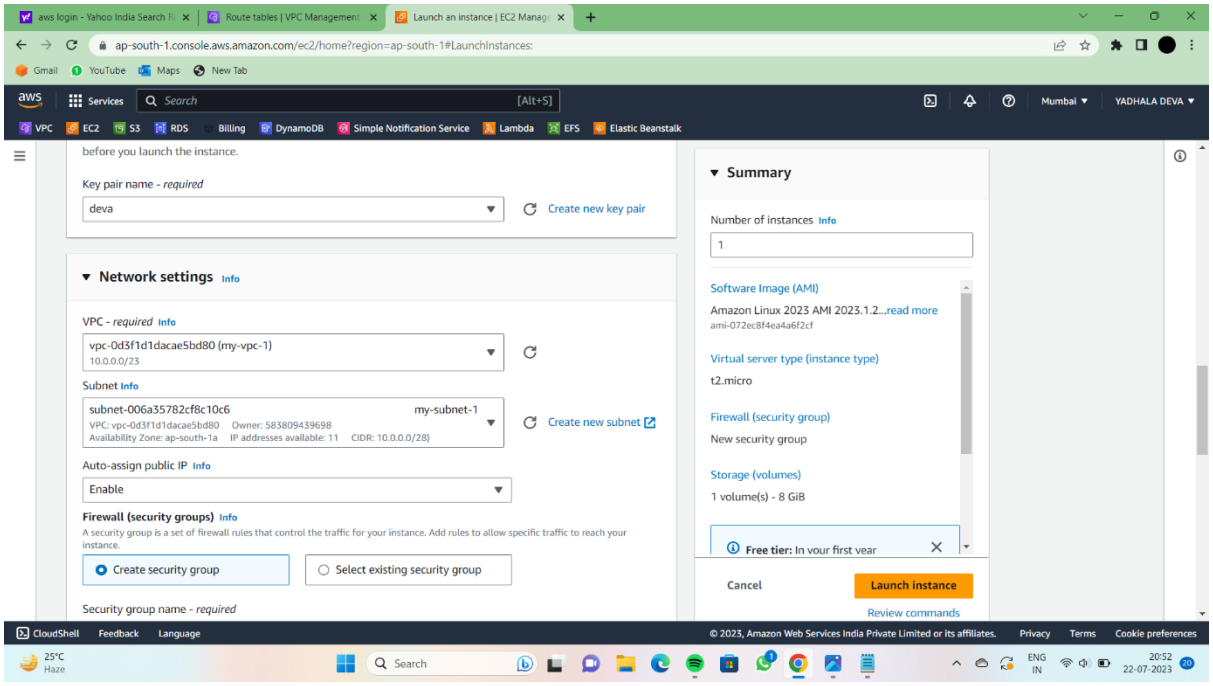

- Go to route tables,select the public route table , and go to routes and click on edit routes and add route and click on save changes.

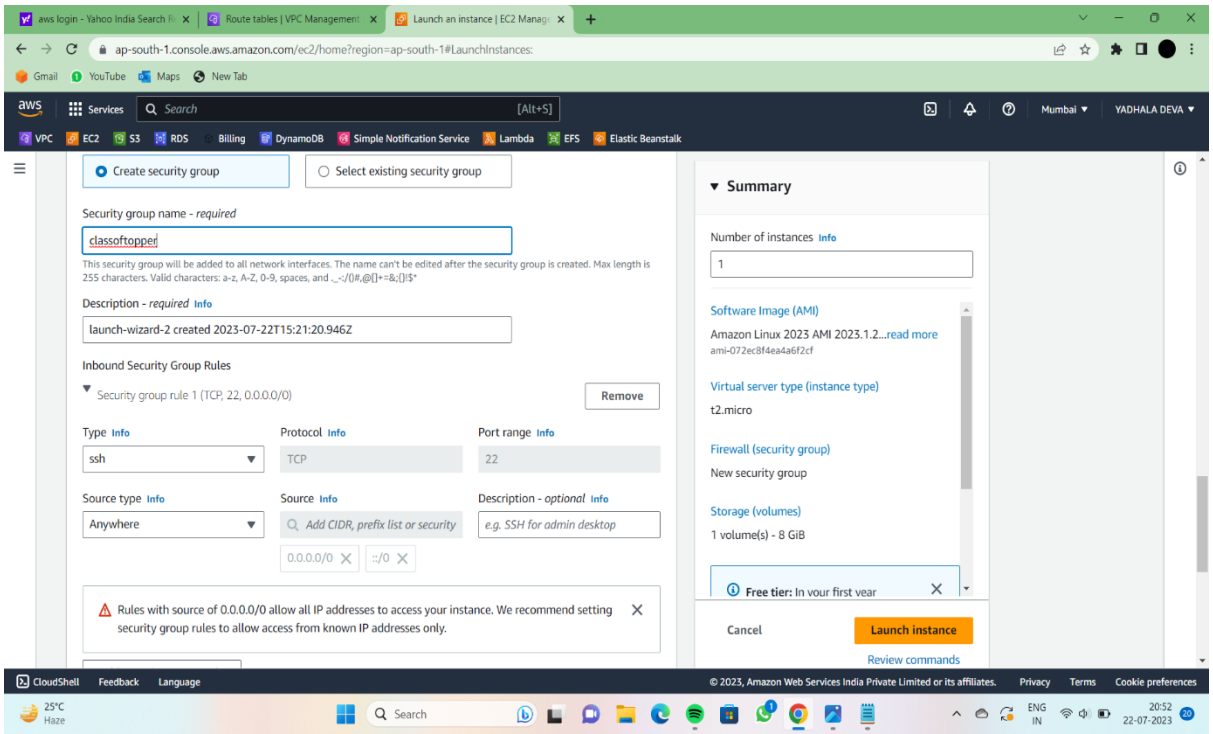


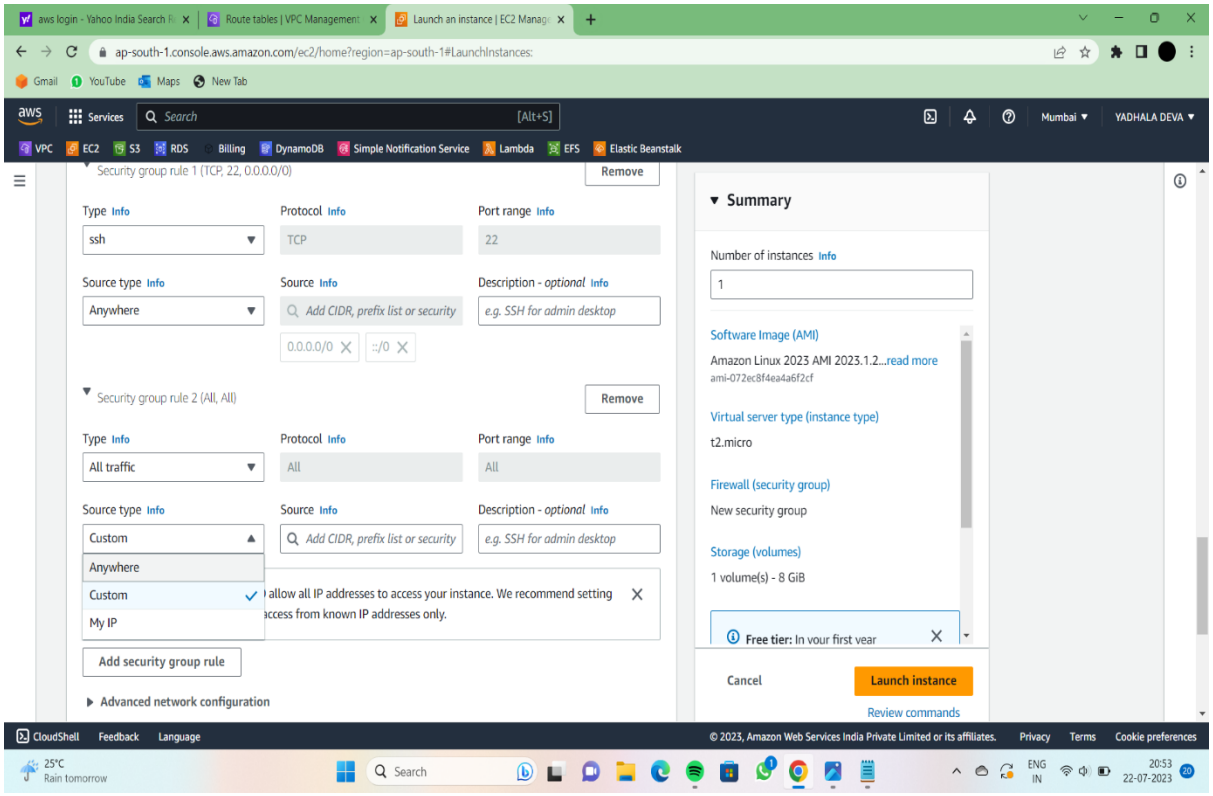
## Service 2 : EC2

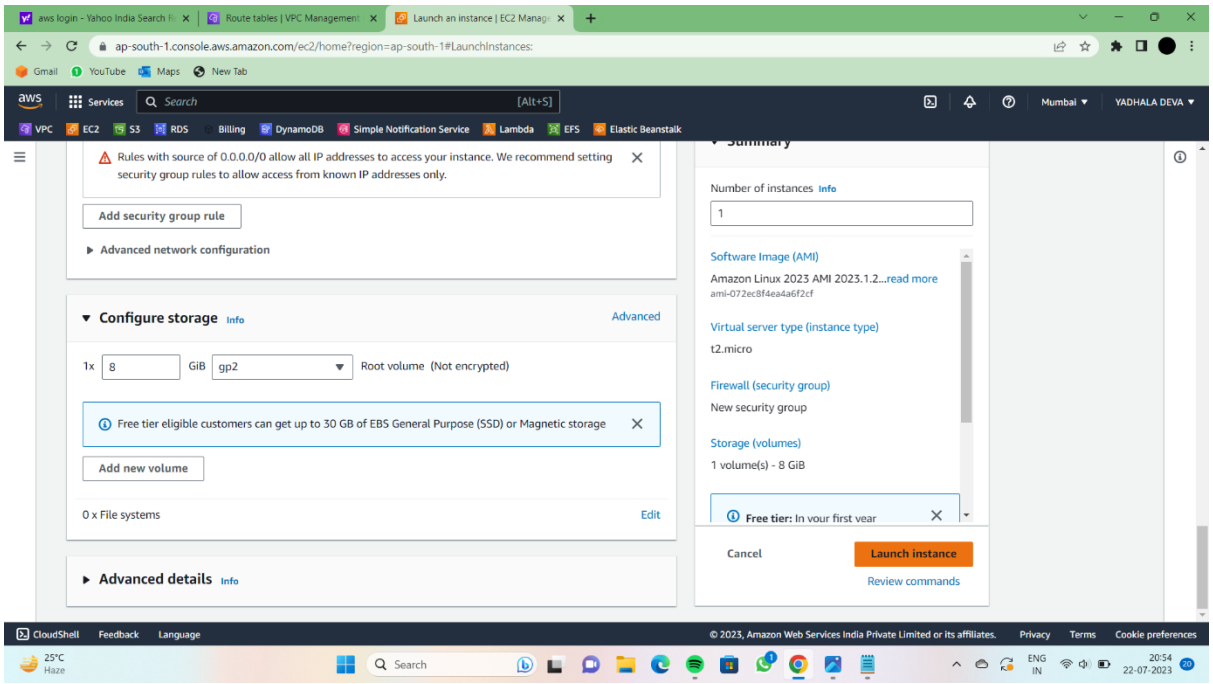
- Creating an EC2 instance in a public subnet as a Bastion Host:
- Name your instance as public instance,
- Select “Amazon Linux 2 AMI”.
- Instance type “t2. micro”.
- Select your existing key pair.
- Select your custom VPC, public subnet and enable the auto-assign public IP.
- In the security group section, select availability zone as south-1a.
- create a new security group, add security groups that supports SSH and all the traffic.
- Launch your instance.

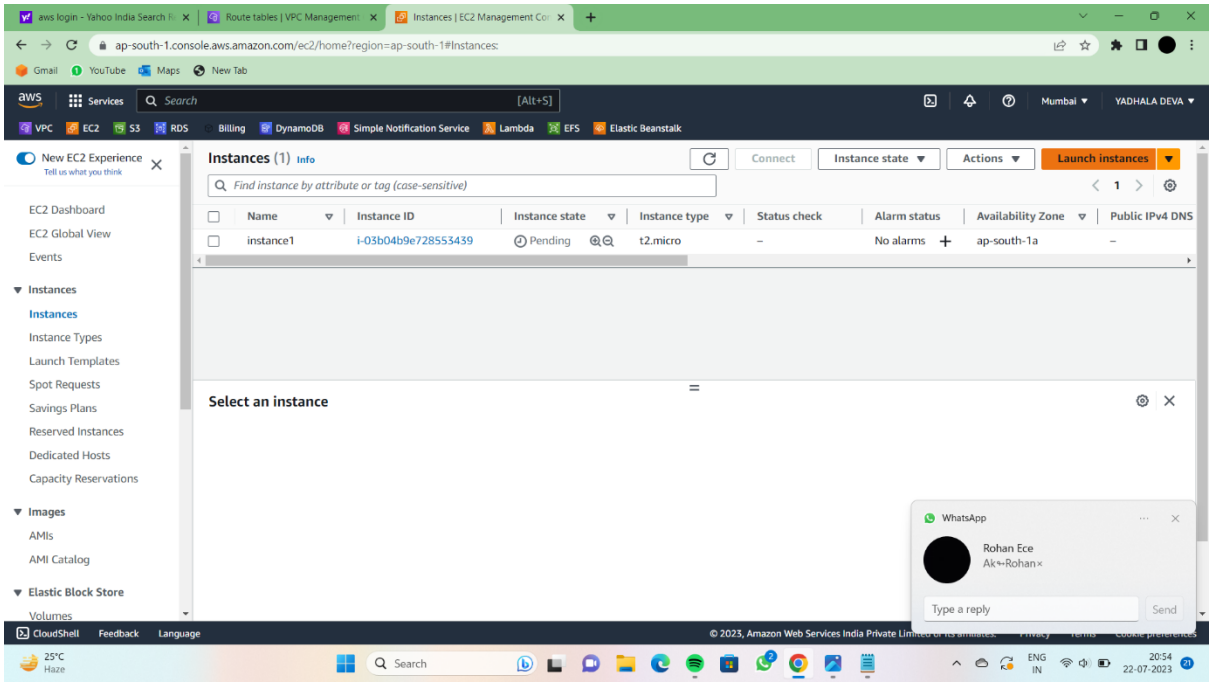

aws login - Yahoo India Search R
Route tables | VPC Management
Launch an instance | EC2 Manage
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
Gmail
YouTube
Maps
New Tab
aws
Services
Search
[Alt+S]
Mumbai
YADHALA DEVA
VPC
EC2
S3
RDS
Billing
DynamoDB
Simple Notification Service
Lambda
EFS
Elastic Beanstalk
Launch an instance Info
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags Info
Name
instance1
Add additional tags
Application and OS Images (Amazon Machine Image) Info
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below
Search our full catalog including 1000s of application and OS images
Quick Start
Amazon
macOS
Ubuntu
Windows
Red Hat
SUSE Li
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.1.2...read more
ami-072ec8f4ea4a6f2cf
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year
Cancel
Launch instance
Review commands
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
25°C
Haze
Search
ENG
IN
20:51
22-07-2023


Key pair name - required
deva
Create new key pair
Network settings Info
VPC - required Info
vpc-0d3f1d1dacae5bd80 (my-vpc-1)
10.0.0.0/23
Subnet Info
subnet-006a35782cf8c10c6 my-subnet-1
Create new subnet
Auto-assign public IP Info
Enable
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
Security group name - required
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.1.2...read more
ami-072ec8f4ea4a6f2cf
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year
Cancel
Launch instance
Review commands

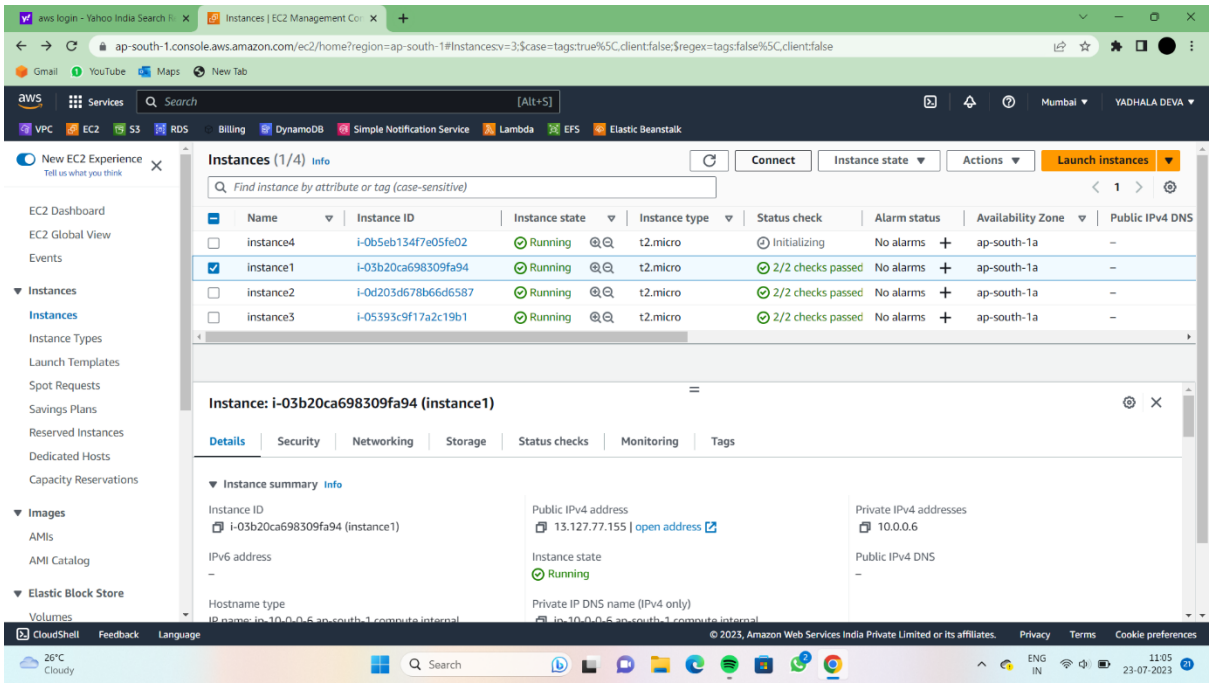

Create security group
Select existing security group
Security group name - required
classoftopper
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*
Description - required Info
launch-wizard-2 created 2023-07-22T15:21:20.946Z
Inbound Security Group Rules
Security group rule 1 (TCP, 22, 0.0.0.0/0)
Remove
Type Info
ssh
Protocol Info
TCP
Port range Info
22
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or security
Description - optional Info
e.g. SSH for admin desktop
0.0.0.0/0
::/0
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.1.2...read more
ami-072ec8f4ea4a6f2cf
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year
Cancel
Launch instance
Review commands


Security group rule 1 (TCP, 22, 0.0.0.0/0)
Remove
Type Info
ssh
Protocol Info
TCP
Port range Info
22
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or security
Description - optional Info
e.g. SSH for admin desktop
0.0.0.0/0
::/0
Security group rule 2 (All, All)
Remove
Type Info
All traffic
Protocol Info
All
Port range Info
All
Source type Info
Custom
Source Info
Add CIDR, prefix list or security
Description - optional Info
e.g. SSH for admin desktop
Anywhere
Custom
My IP
allow all IP addresses to access your instance. We recommend setting
access from known IP addresses only.
Add security group rule
Advanced network configuration
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.1.2...read more
ami-072ec8f4ea4a6f2cf
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year
Cancel
Launch instance
Review commands
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

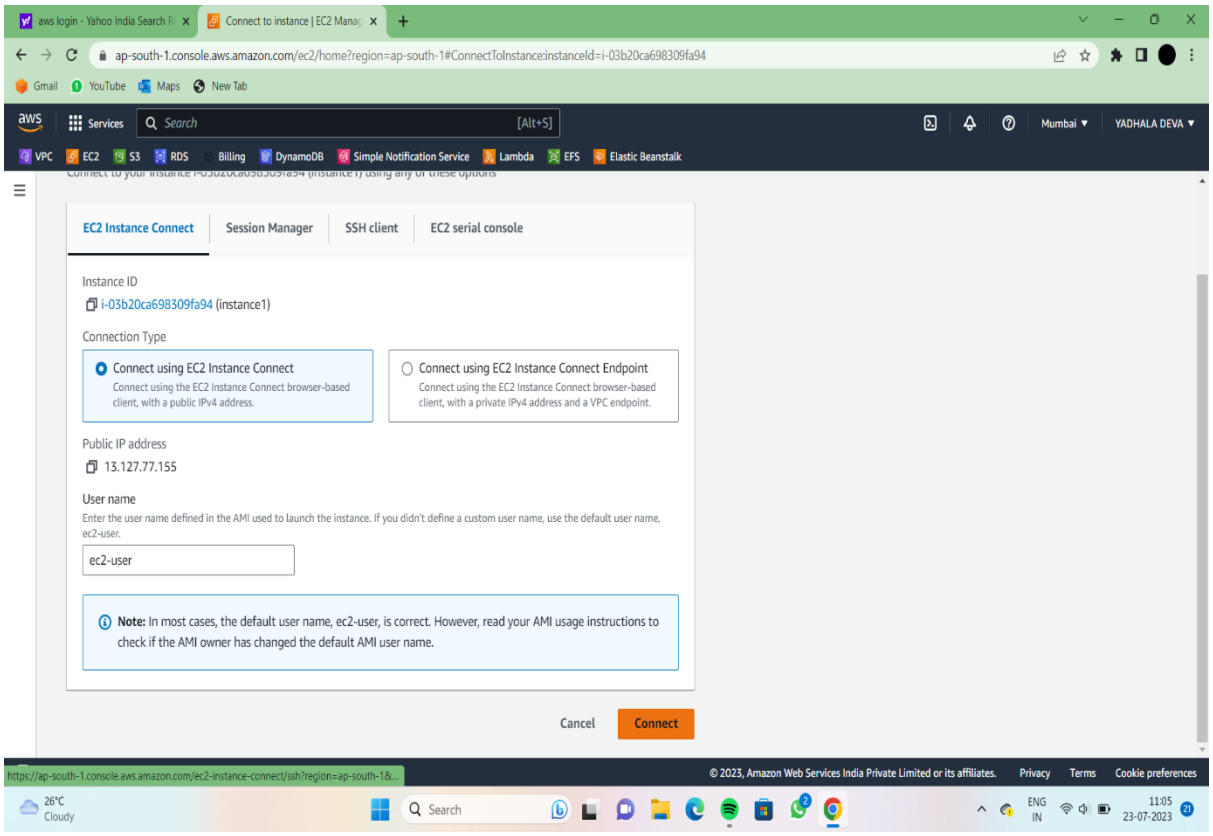

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Add security group rule
Advanced network configuration
Configure storage Info
Advanced
1x
8
GiB
gp2
Root volume (Not encrypted)
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage
Add new volume
0 x File systems
Edit
Advanced details Info
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.1.2...read more
ami-072ec8f4ea4a6f2cf
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year
Cancel
Launch instance
Review commands
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

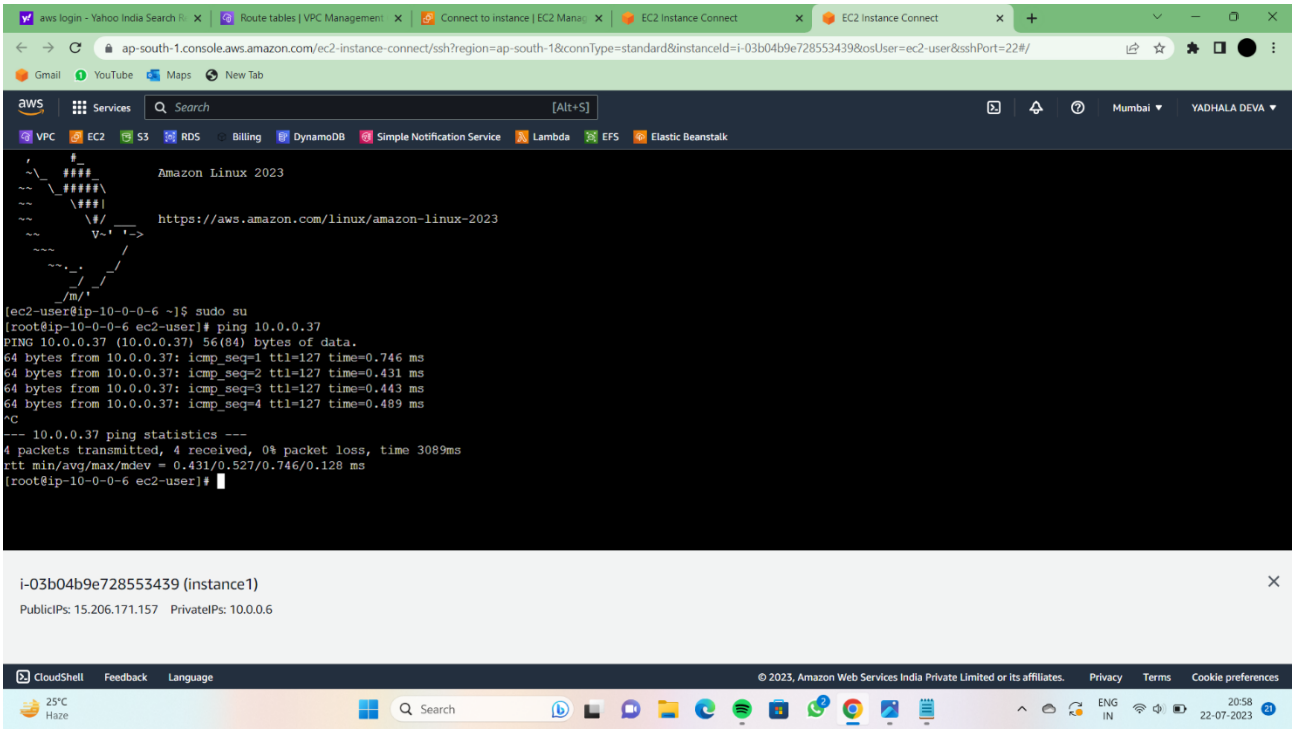


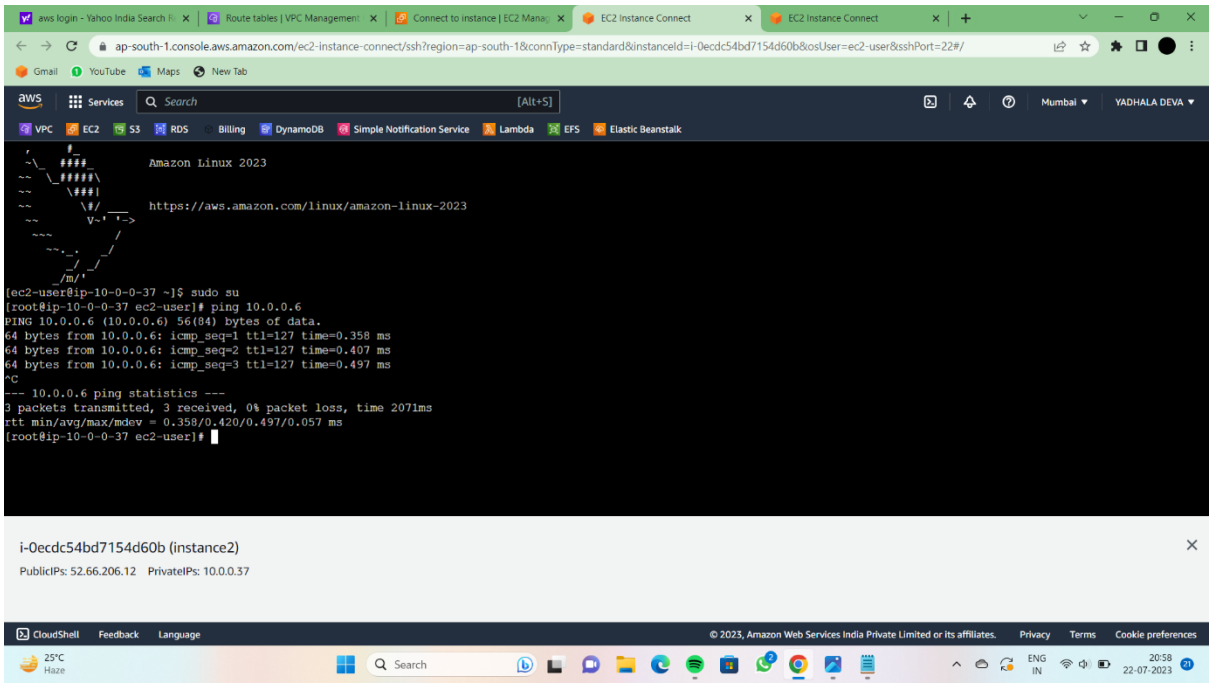

- Instance-1 is created.
- As well as we have to create another three instances-instance-2,instance-3,instance-4.



- Now connect instance-1 and instance-2.

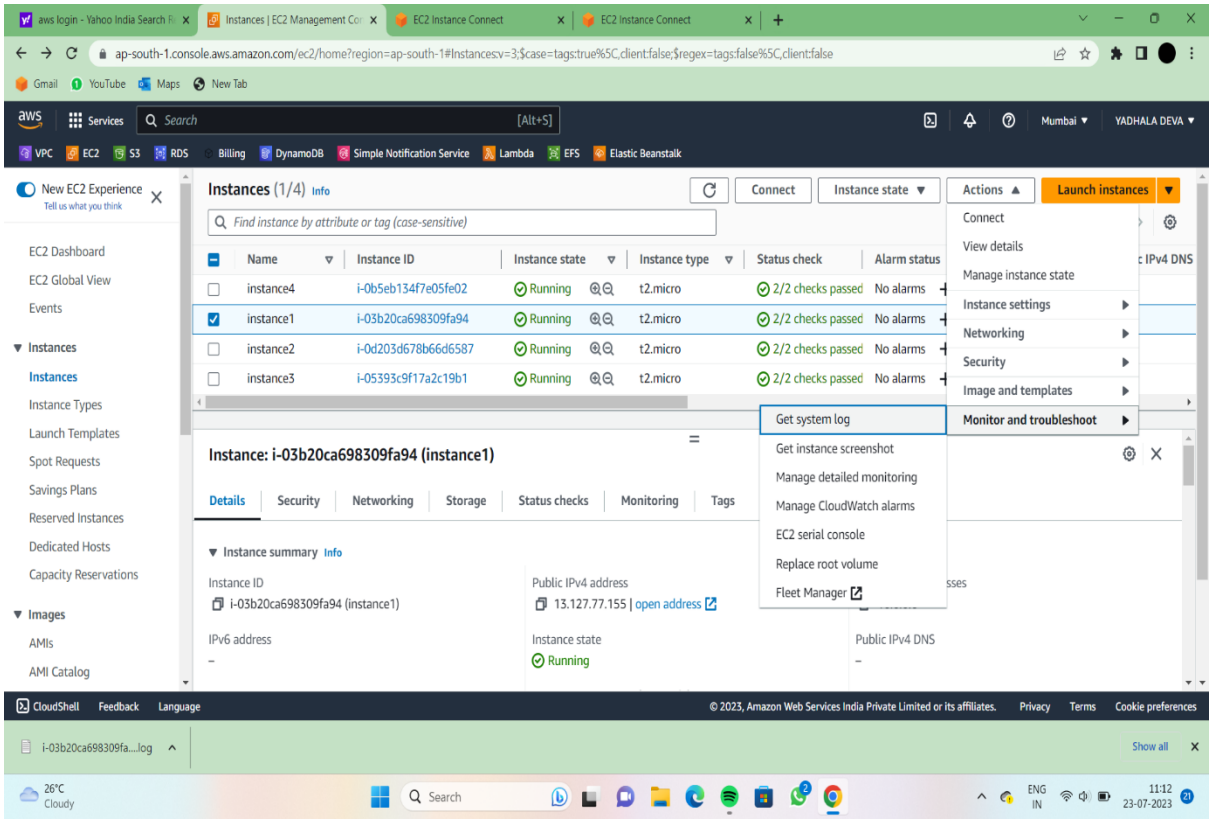




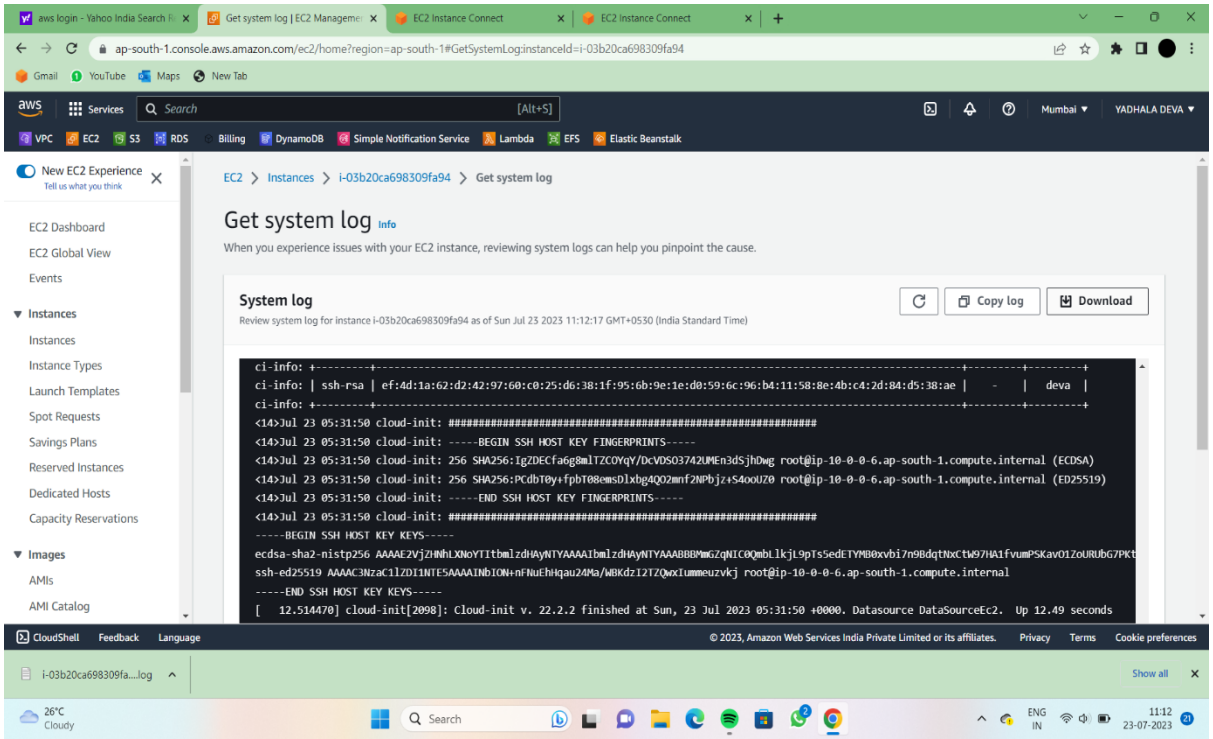




- In above pictures pinging is done between instance-1 and instance-2.
- Select instance-1 and click on actions.

- Next click on Monitor and troubleshoot.
- Then click on get system log.

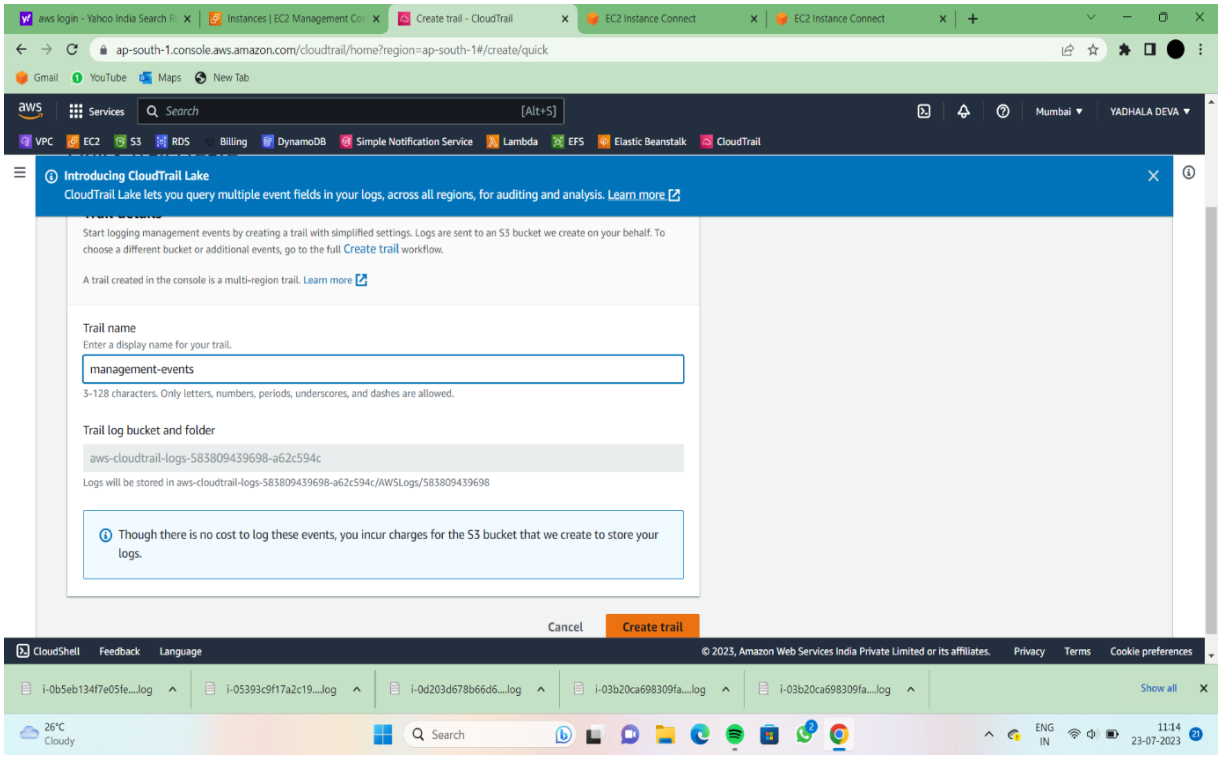


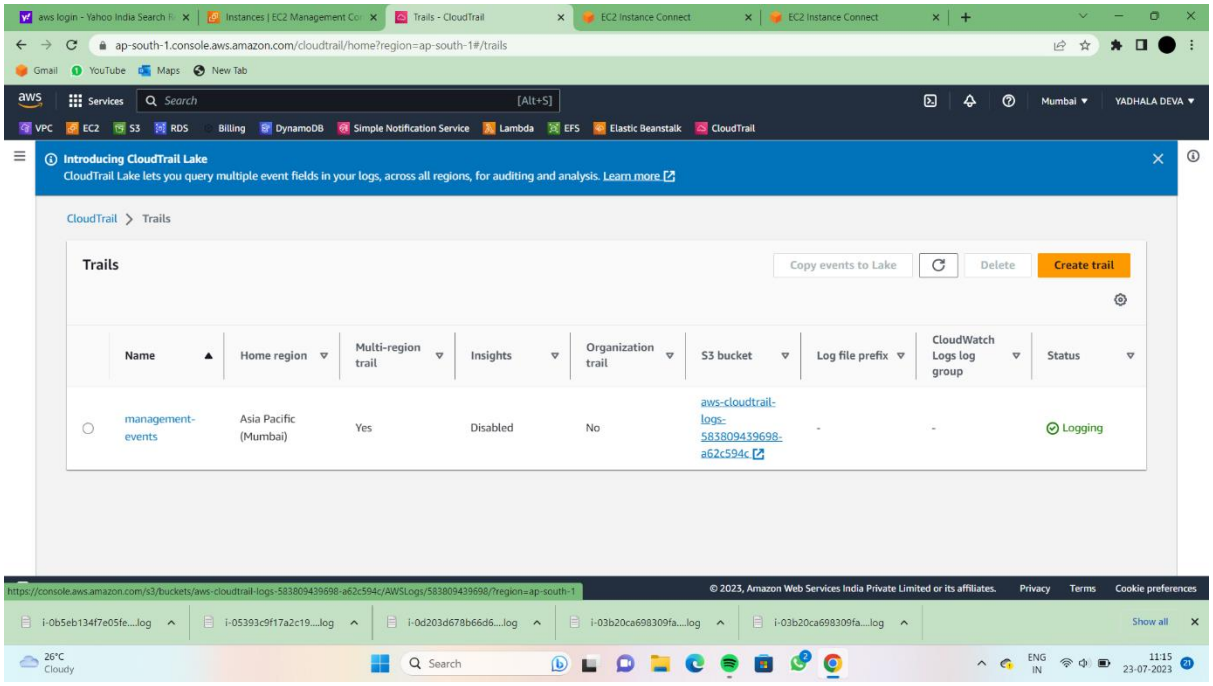

- Then download the system log code.



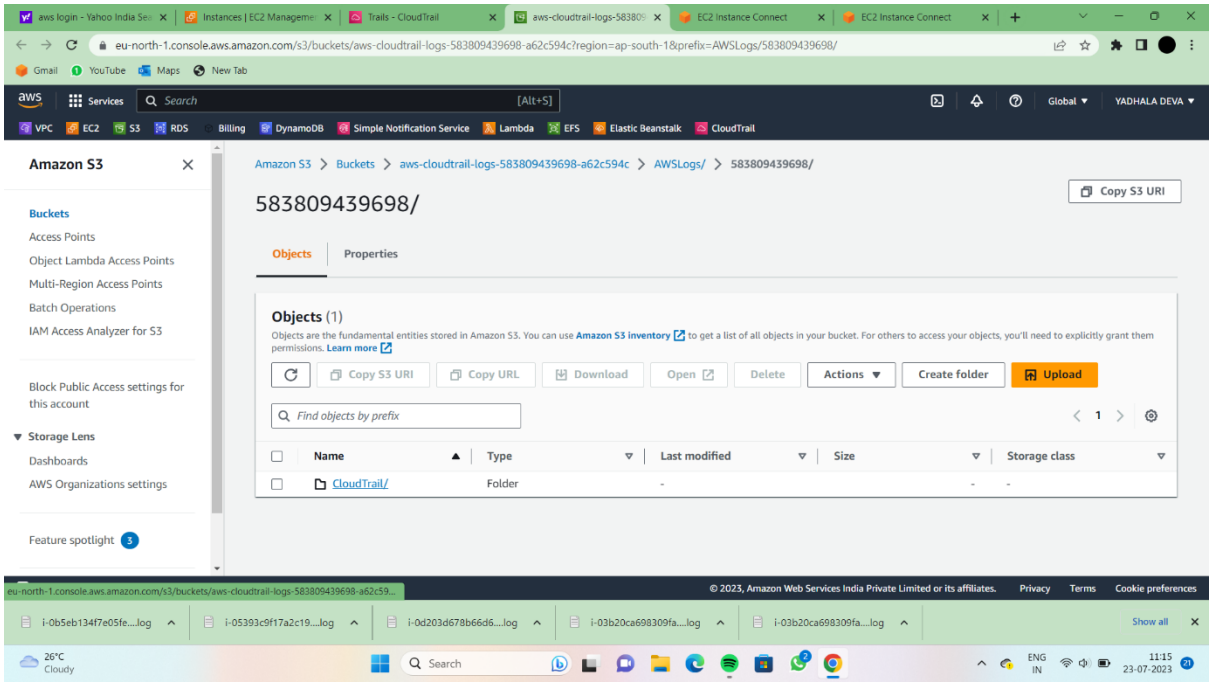
**Service 3** : Implementing CloudTrail for Auditing

- Go to the AWS Management Console.
- Navigate to the CloudTrail service.
- Click "Create Trail."
- Configure the trail:
- Specify the trail name.
- Choose whether you want to apply the trail to all regions or specific regions.
- Select an existing S3 bucket or create a new one to store the logs.
- (Optional) Define log file encryption and cloud watch logs settings.
- Click "Create."

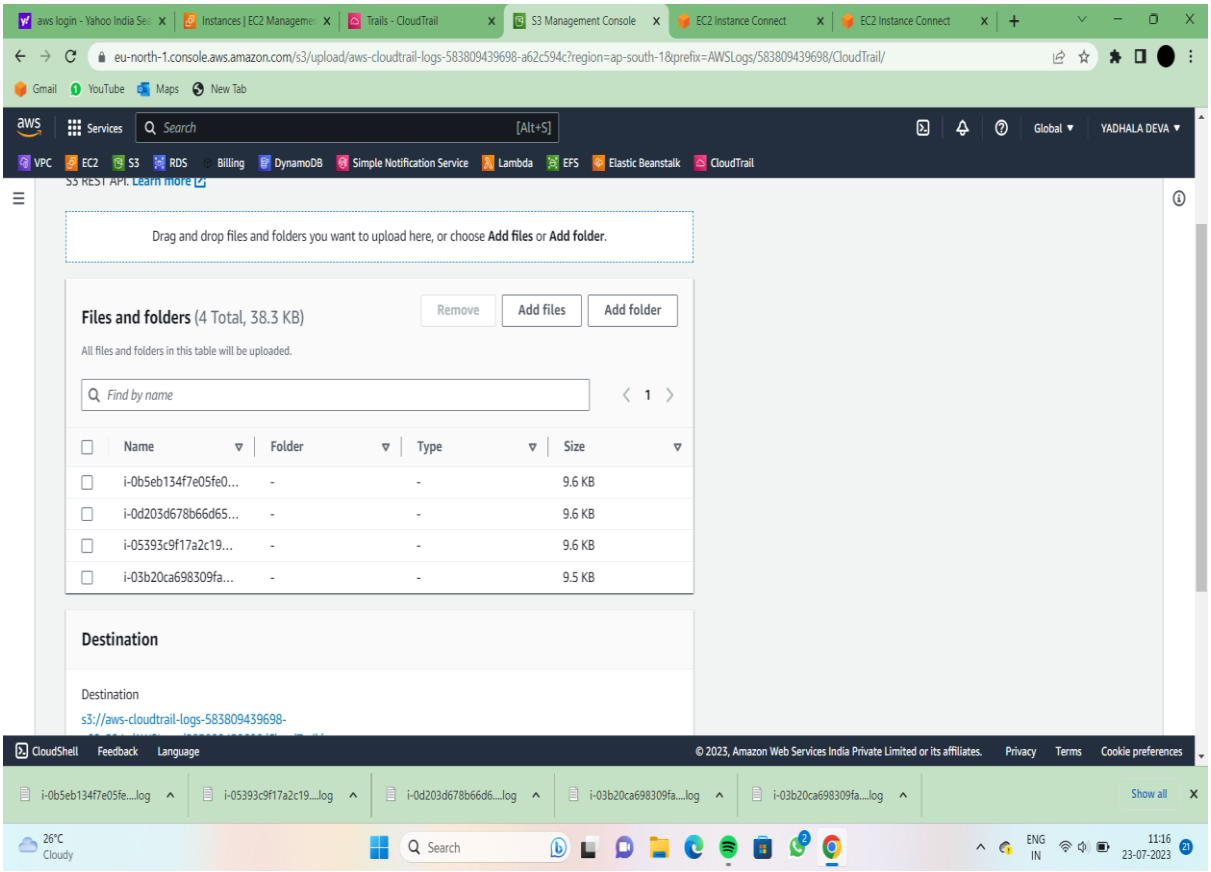




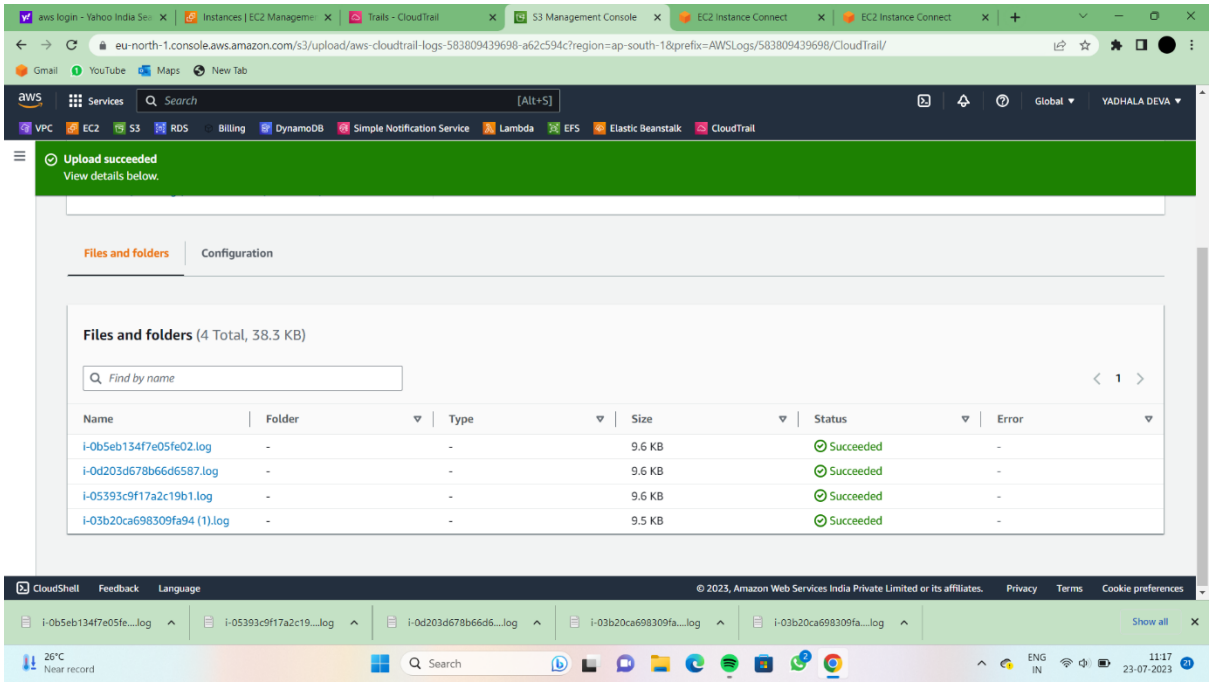

- Go to Amazon S3 and click on buckets .
- Then click on bucket name.




- Now click on upload.

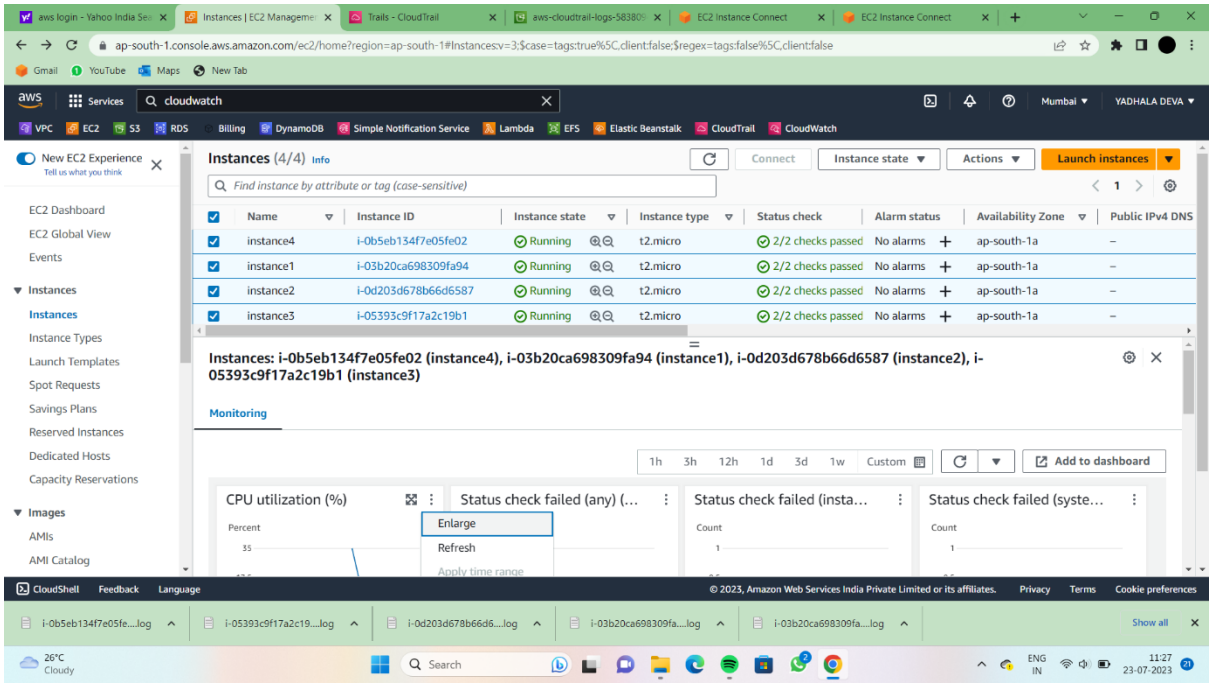


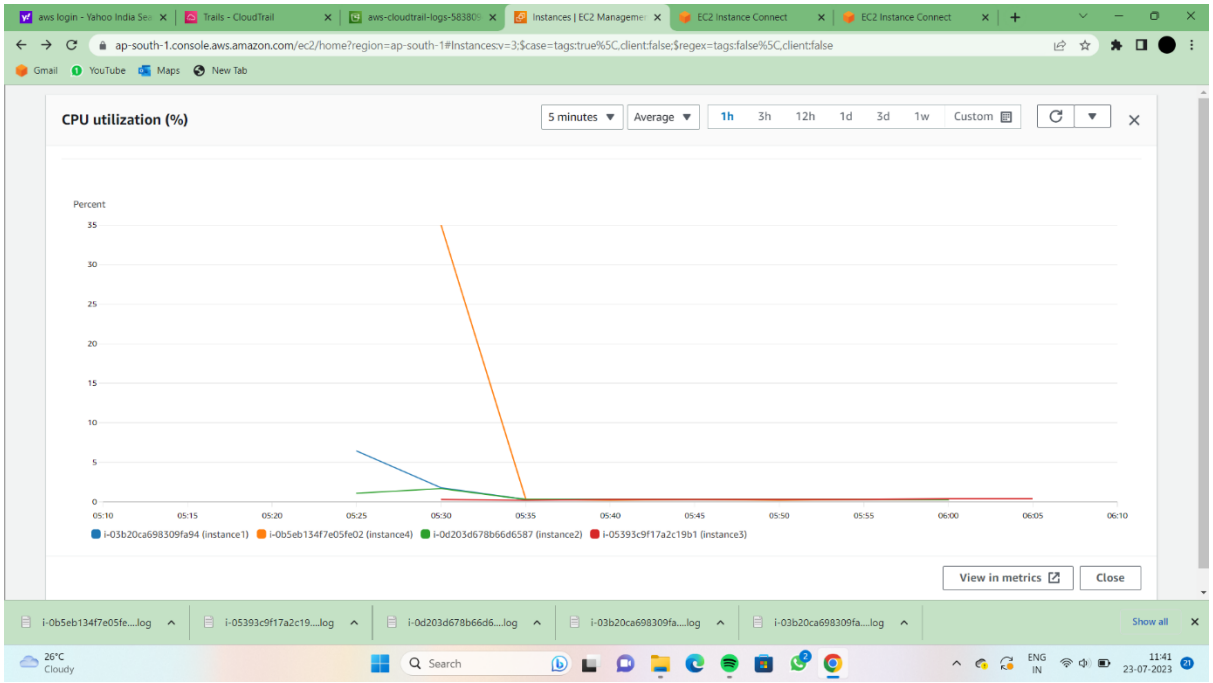

- In above picture ,we add files of four system log codes.

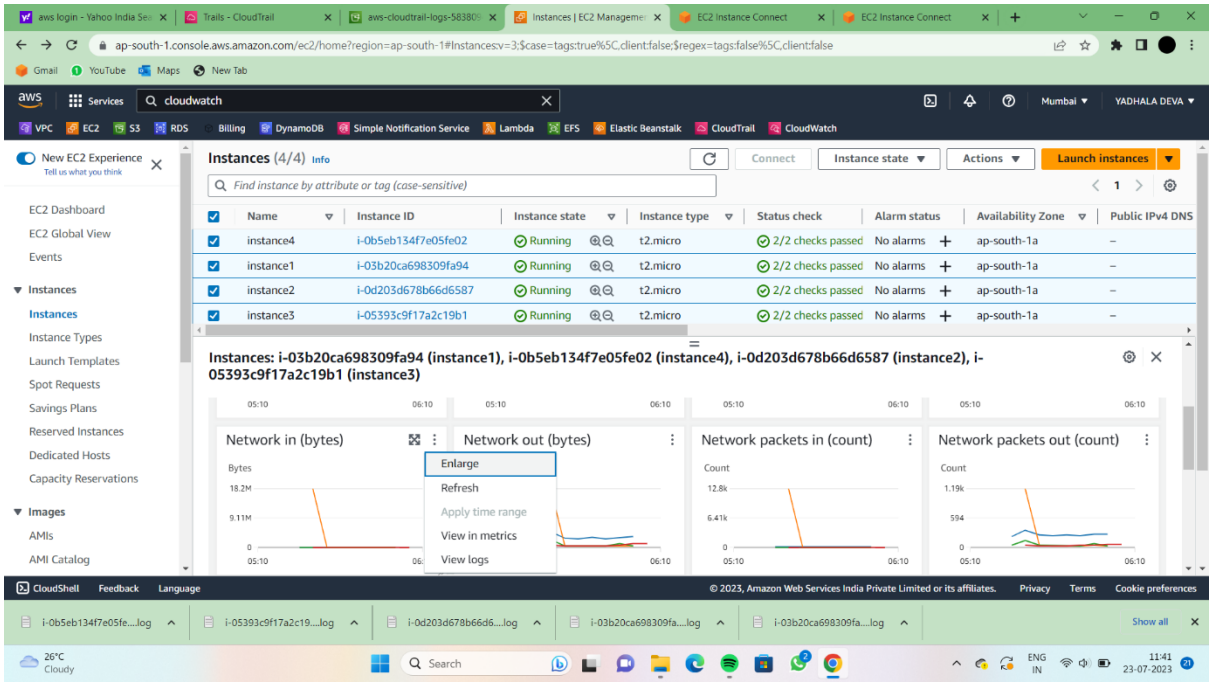


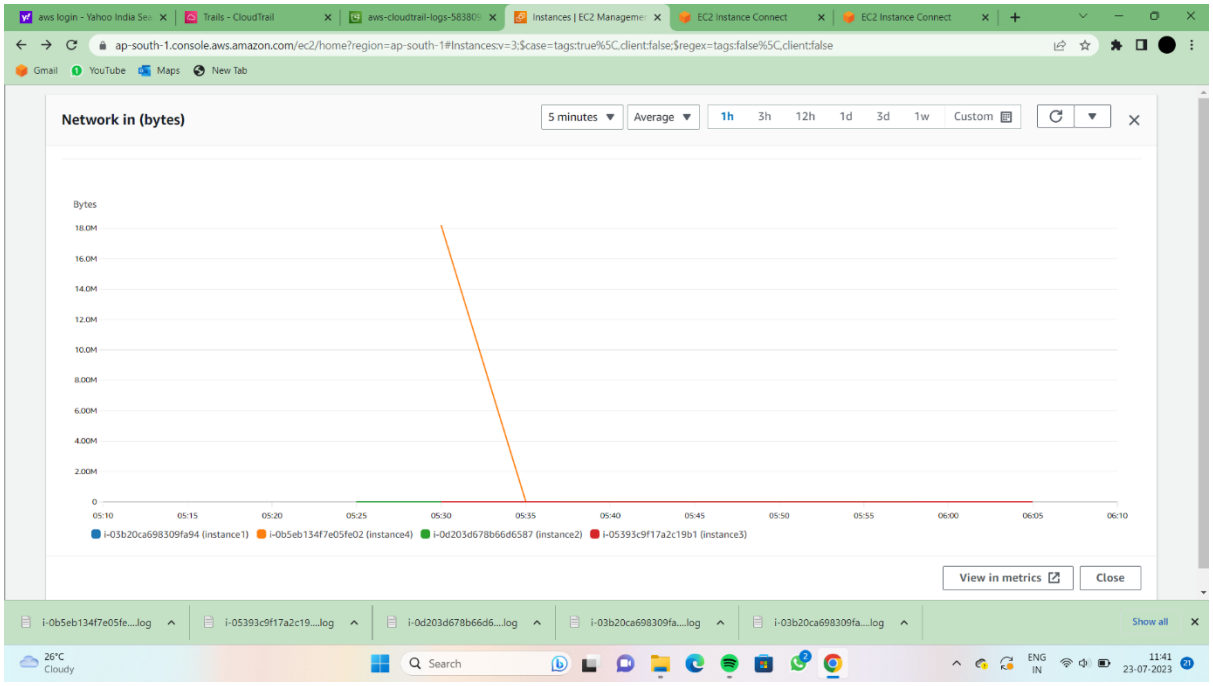
Service 4 : AWS CloudWatch

- Click on "Metrics" in the left-hand navigation pane.
- Choose the AWS service you want to monitor (e.g., EC2, RDS, S3).
- Select the metric you want to view.
- Customize the graph settings (e.g., time range, statistic).
- Click on the "Create alarm" button to create an alarm directly from the metric.




CPU utilization (%)
5 minutes
Average
1h
3h
12h
1d
3d
1w
Custom
Percent
35
30
25
20
15
10
5
0
05:10
05:15
05:20
05:25
05:30
05:35
05:40
05:45
05:50
05:55
06:00
06:05
06:10
i-03b20ca698309fa94 (instance1)
i-0b5eb134f7e05fe02 (instance4)
i-0d203d678b66d6587 (instance2)
i-05393c9f17a2c19b1 (instance3)
View in metrics
Close


cloudwatch
Instances (4/4) Info
Connect
Instance state
Actions
Launch instances
Find instance by attribute or tag (case-sensitive)
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
instance4 i-0b5eb134f7e05fe02 Running t2.micro 2/2 checks passed No alarms ap-south-1a
instance1 i-03b20ca698309fa94 Running t2.micro 2/2 checks passed No alarms ap-south-1a
instance2 i-0d203d678b66d6587 Running t2.micro 2/2 checks passed No alarms ap-south-1a
instance3 i-05393c9f17a2c19b1 Running t2.micro 2/2 checks passed No alarms ap-south-1a
Instances: i-03b20ca698309fa94 (instance1), i-0b5eb134f7e05fe02 (instance4), i-0d203d678b66d6587 (instance2), i-05393c9f17a2c19b1 (instance3)
Network in (bytes)
Network out (bytes)
Network packets in (count)
Network packets out (count)
Enlarge
Refresh
Apply time range
View in metrics
View logs
EC2 Dashboard
EC2 Global View
Events
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog




## Conclusion :

In conclusion, this project aims to demonstrate the process of building a robust architectural infrastructure using AWS VPC with 20 subnets, ensuring security through CloudTrail auditing, and enabling proactive monitoring with CloudWatch. By successfully implementing this infrastructure, we can achieve a secure, scalable, and resilient cloud environment, setting the foundation for various applications and services with high availability and optimal performance. Through this report, we hope to provide valuable insights and guidelines for future endeavors in architecting similar AWS-based infrastructures.