=

BLACKBUCKS INTERNSHIP REPORT

Performing operations on S3 buckets within an EC2 instance by means of an IAM Role

SUBMITTED BY

VENDRA JAHNAVI (21B95A0530)
MADDIRALA SUPRAJA (20B91A04D1)
SHAIK KARISHMA (20B91A04L8)
VELPURI USHA KRUPA SRI (20B91A04P8)

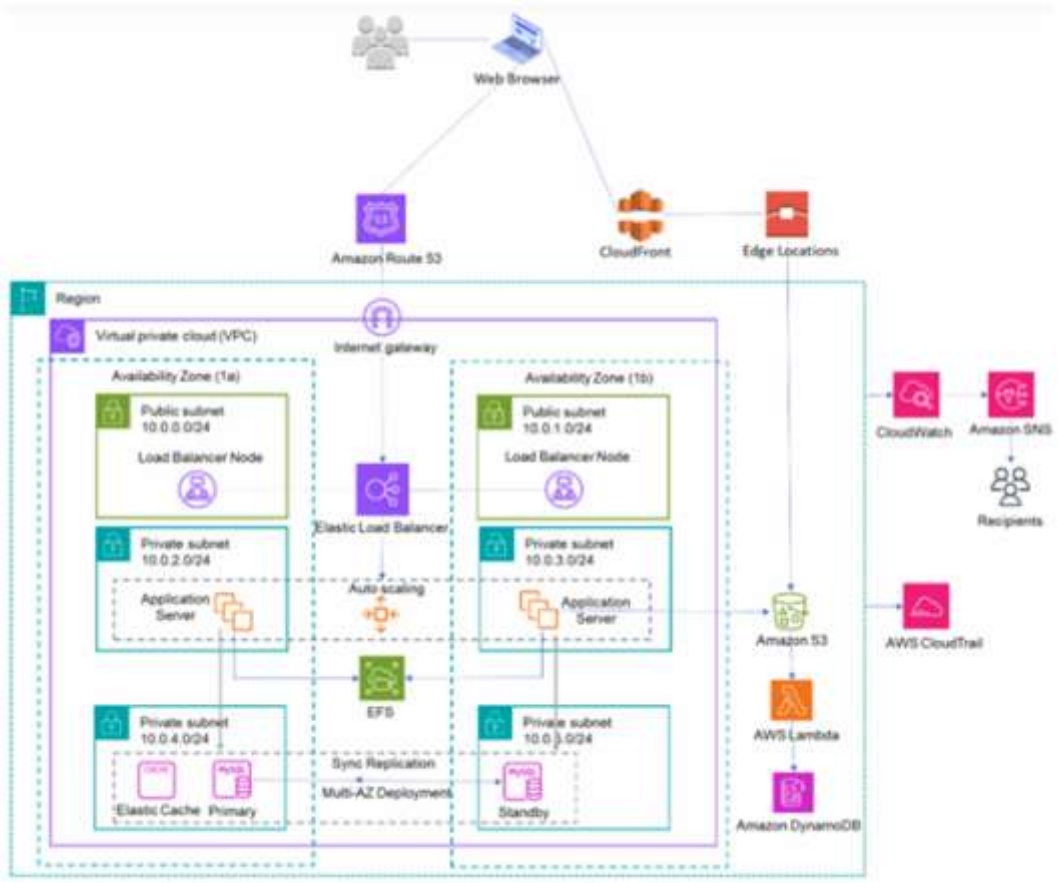
UNDER THE GUIDANCE OF MS. Anupama Voruganti

Blackbuck Engineers Pvt. Ltd

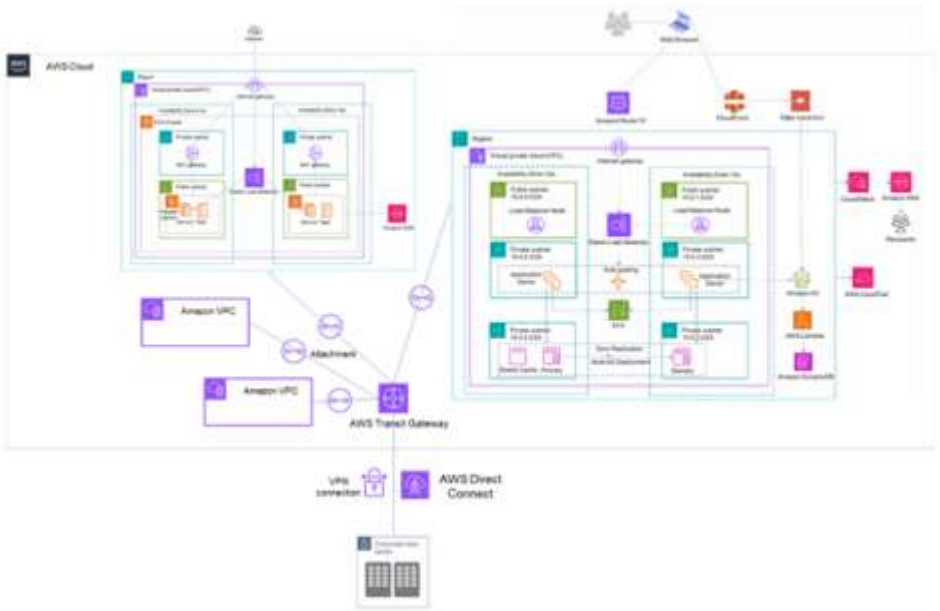
Road No 36, Jubilee Hills, Hyderabad

AWS Services acquired during this internship program

AWS Services acquired during this internship program (Initial Architecture)



AWS Services acquired during this internship program (Complete architecture)



Services used in this internship:

EC2: Amazon Elastic Compute Cloud (EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is a powerful tool that can be used to run a wide variety of applications, including web servers, databases, and big data processing applications.EC2 instances are virtual servers that can be launched in minutes. You can choose from a variety of instance types, each with different configurations of CPU, memory, storage, and networking capacity.
S3: Amazon Simple Storage Service (S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere. S3 is a great way to store static content for web sites and applications.S3 can be used to store backups of data from on-premises systems.

EFS: Amazon Elastic File System (EFS) is a fully managed file storage service that makes it easy to set up, use, and scale file storage for your Amazon EC2 instances. It is a highly scalable, durable, and secure file storage service that can be used for a variety of workloads. EFS is a serverless service, which means that you do not need to provision or manage any file servers. EFS automatically scales to meet your needs, and you only pay for the storage you use.

VPC: A virtual private cloud (VPC) is a virtual network that you can create in the AWS Cloud. It is a logical isolation of your AWS resources from other AWS resources in the same region. A VPC is a great way to improve the security of your AWS resources. A VPC provides a layer of isolation between your AWS resources and other AWS resources in the same region. This can help to improve the security of your AWS resources.

RDS: Amazon Relational Database Service (RDS) is a fully managed database service that makes it easy to set up, operate, and scale a relational database in the cloud. RDS supports a wide range of popular database engines, including MySQL, PostgreSQL, MariaDB, Oracle, and SQL Server. : RDS takes care of all the details of setting up and configuring your database, so you can focus on your application.

IAM: AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access. IAM can be used to manage users and permissions in AWS. This can help to ensure that only authorized users have access to AWS resources.

CLOUDWATCH: Amazon CloudWatch is a monitoring service for Amazon Web Services (AWS) cloud resources and the applications you run on AWS. CloudWatch collects metrics, logs, and events from your AWS resources and stores them in a central repository.CloudWatch can collect metrics from a wide range of AWS resources, including EC2 instances, EBS volumes, RDS databases, and CloudFront distributions. You can use these metrics to track the performance of your resources and identify potential problems.

Team Members:

- VENDRA JAHNAVI (21B95A0530)
- MADDIRALA SUPRAJA (20B91A04D1)
- SHAIK KARISHMA (20B91A04L8)
- VELPURI USHA KRUPA SRI (20B91A04P8)

Title:

Performing operations on S3 buckets within an EC2 instance by means of an IAM Role

Abstract:

The project focuses on enabling seamless interaction between Amazon Simple Storage Service (S3) buckets and Amazon Elastic Compute Cloud (EC2) instances using Identity and Access Management (IAM) roles. By leveraging IAM roles, the project aims to eliminate the need for access key management and enhance security while performing operations on S3 buckets from within EC2 instances.

IAM roles provide a secure and efficient way to grant permissions to EC2 instances without the need for explicit access keys. The project outlines a step-by-step process to set up an IAM role, attach the necessary policies for S3 bucket access, and launch an EC2 instance with the assigned IAM role.

Once the EC2 instance is launched with the IAM role, the project describes how to access the instance and configure the AWS CLI or SDKs to utilize the temporary credentials provided by the IAM role. This configuration enables developers to interact with S3 buckets directly from the EC2 instance, performing operations such as listing bucket contents, uploading files, or downloading data.

By adopting IAM roles for S3 bucket operations within EC2 instances, the project emphasizes enhanced security, as access keys are not exposed or stored on the instance. The automatic provisioning of temporary credentials through IAM roles simplifies the management process and aligns with best practices for secure access control.

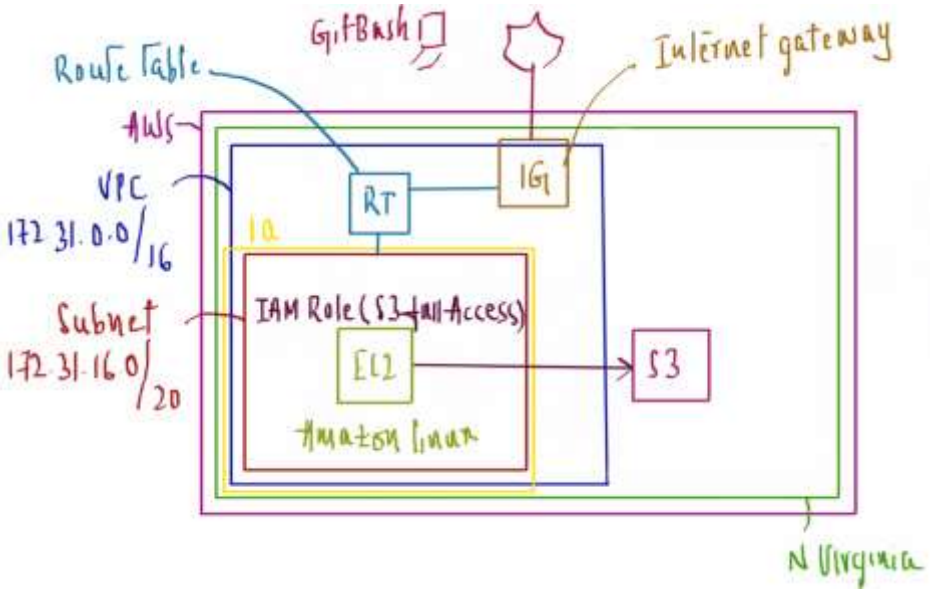
Overall, the project provides a comprehensive guide on utilizing IAM roles to integrate S3 bucket operations within EC2 instances, empowering developers to securely and efficiently interact with S3 data from within their EC2 environments.

TABLE OF CONTENTS

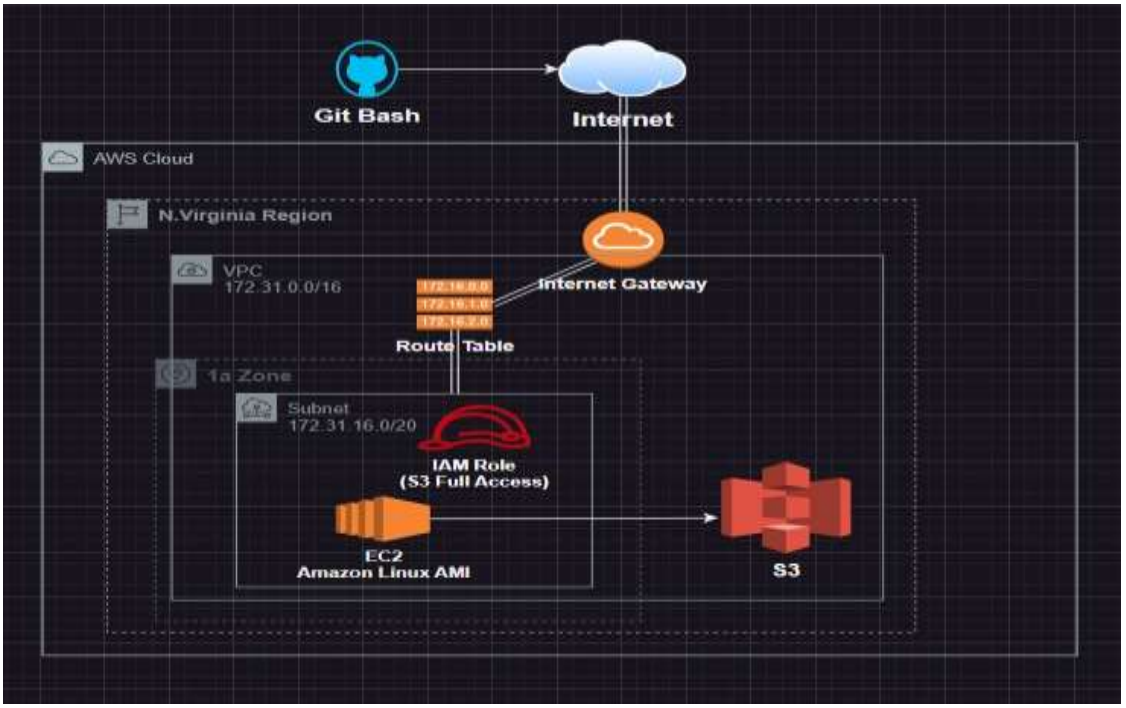
Services used in the project -

- S3 (Simple Storage Service)
- IAM (Identity and Access Management)
- EC2 (Elastic Compute Cloud)

Skeleton architecture -



Terminal Blueprint –



Introduction to Cloud Computing:

Cloud computing is on-demand access, via the internet, to computing resources—applications, servers (physical servers and virtual servers), data storage, development tools, networking capabilities, and more—hosted at a remote data center managed by a cloud services provider (or CSP). The CSP makes these resources available for a monthly subscription fee or bills them according to usage.

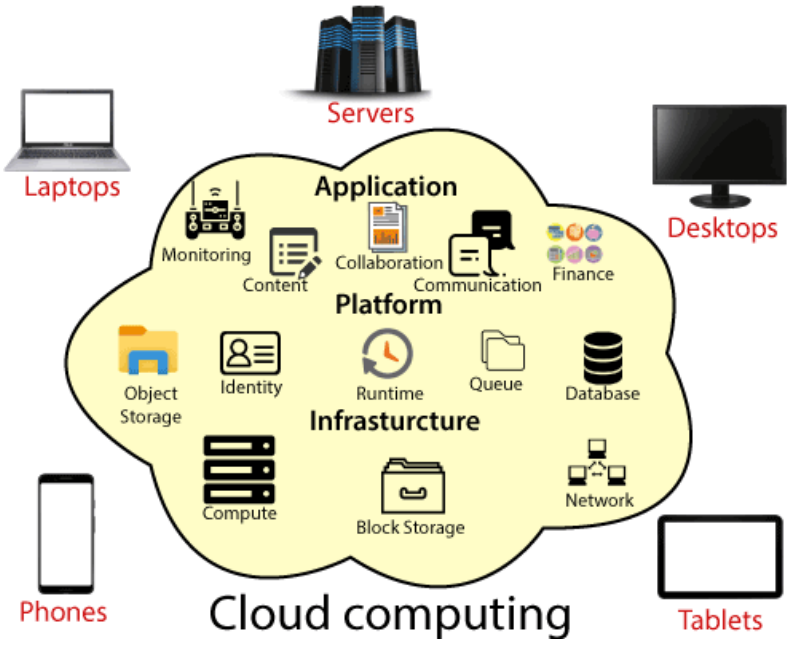
Compared to traditional on-premises IT, and depending on the cloud services you select, cloud computing helps do the following:

• **Lower IT costs**: Cloud lets you offload some or most of the costs and effort of purchasing, installing, configuring, and managing your own on-premises infrastructure.

• **Improve agility and time-to-value:** With the cloud, your organization can start using enterprise applications in minutes, instead of waiting weeks or months for IT to respond to a request, purchase and configure supporting hardware, and install software. Cloud also lets you empower certain users—specifically developers and data scientists.

• **Scale more easily and cost-effectively:** Cloud provides elasticity—instead of purchasing excess capacity that sits unused during slow periods, you can scale capacity up and down in response to spikes and dips in traffic. You can also take advantage of your cloud provider's global network to spread your applications closer to users around the world.

The term 'cloud computing' also refers to the technology that makes the cloud work. This includes some form of virtualized IT infrastructure—servers, operating system software, networking, and other infrastructure that's abstracted, using special software, so that it can be pooled and divided irrespective of physical hardware boundaries. For example, a single hardware server can be divided into multiple virtual servers.



Advantages of Cloud:

Cloud computing offers numerous advantages that have transformed the IT landscape and provided significant benefits to businesses and individuals. Some key advantages of cloud computing include:

1. **Scalability**: Cloud computing allows organizations to scale their resources up or down quickly based on demand. This scalability ensures that businesses have the necessary computing power and storage capacity to handle fluctuations in workload without the need for upfront investments in infrastructure.

2. **Cost Savings:** Cloud computing eliminates the need for organizations to invest in and maintain their own physical infrastructure. Instead, they can pay for the resources they actually use on a pay-as-you-go basis. This reduces upfront capital expenditure and ongoing operational costs associated with hardware procurement, maintenance, and upgrades.

3. **Flexibility and Agility:** Cloud services provide organizations with the flexibility to experiment, innovate, and deploy applications and services quickly. Development teams can access the necessary resources and tools without delays, enabling faster time-to-market and the ability to respond rapidly to changing business needs.

4. **Reliability and Availability:** Cloud providers typically offer robust infrastructure with redundant systems and data replication, ensuring high levels of reliability and availability. This means that applications and data are accessible even in the event of hardware failures or disruptions, providing businesses with enhanced continuity and minimizing downtime.

5. **Global Accessibility:** Cloud services can be accessed from anywhere in the world with an internet connection. This global accessibility enables remote work, collaboration among geographically dispersed teams, and seamless data sharing across locations.

6. **Security:** Cloud providers invest heavily in security measures to protect data and infrastructure. They employ advanced security technologies, encryption techniques, and compliance frameworks to ensure the confidentiality, integrity, and availability of data. Additionally, cloud services offer robust backup and disaster recovery capabilities, enhancing data protection and business continuity.

7. **Innovation and Resource Optimization:** Cloud computing enables organizations to focus on their core competencies and innovation rather than managing IT infrastructure. It provides access to a wide range of tools, technologies, and services that can be leveraged to drive innovation, experiment with new ideas, and optimize resource utilization.

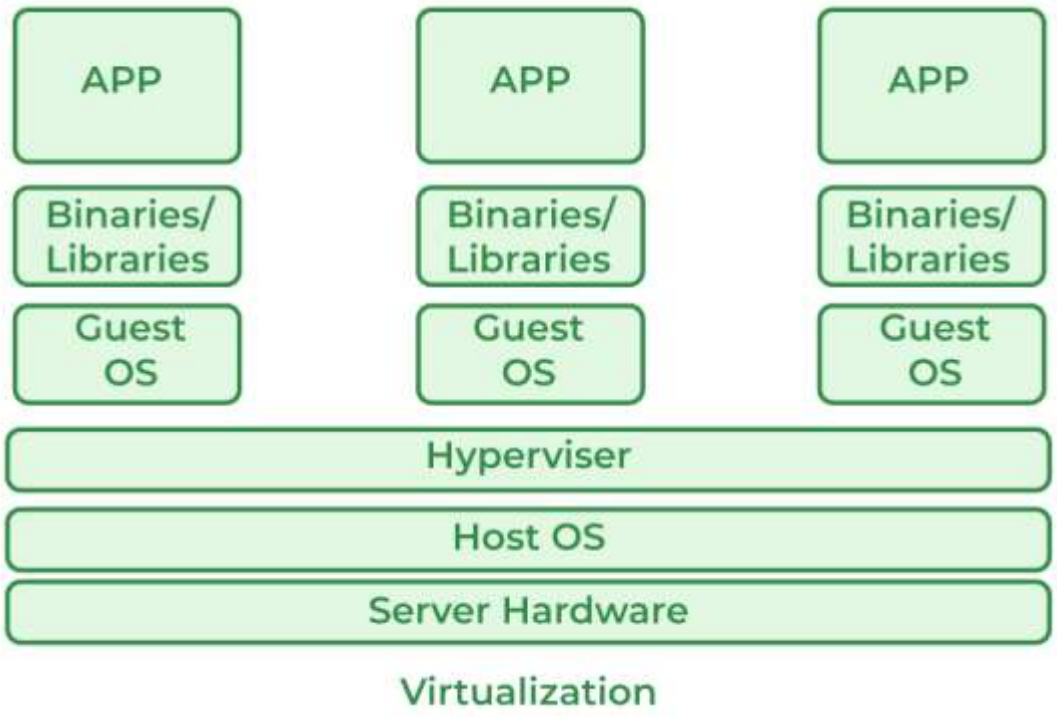
8. **Environmental Sustainability:** Cloud computing promotes environmental sustainability by reducing the need for physical infrastructure and enabling resource sharing among multiple users. It helps to minimize energy consumption, carbon footprint, and electronic waste associated with traditional on-premises data centers.

Overall, cloud computing offers scalability, cost savings, flexibility, reliability, security, and the ability to drive innovation. It has become a foundational technology that empowers businesses to adapt to changing market conditions, accelerate growth, and stay competitive in today's dynamic digital landscape.

Virtualization Architecture:

Virtualization is a technique how to separate a service from the underlying physical delivery of that service. It is the process of creating a virtual version of something like computer hardware. It was initially developed during the mainframe era. It involves using specialized software to create a virtual or software-created version of a computing resource rather than the actual version of the same resource. With the help of Virtualization, multiple operating systems and applications can run on the same machine and its same hardware at the same time, increasing the utilization and flexibility of hardware.

In other words, one of the main cost-effective, hardware-reducing, and energy-saving techniques used by cloud providers is Virtualization. Virtualization allows sharing of a single physical instance of a resource or an application among multiple customers and organizations at one time. It does this by assigning a logical name to physical storage and providing a pointer to that physical resource on demand. The term virtualization is often synonymous with hardware virtualization, which plays a fundamental role in efficiently delivering Infrastructure-as-a-Service (IaaS) solutions for cloud computing. Moreover, virtualization technologies provide a virtual environment for not only executing applications but also for storage, memory, and networking.



Virtualization

The key components of virtualization architecture in cloud computing are:

1. Hypervisor or Virtual Machine Monitor (VMM): The hypervisor is responsible for managing and controlling the virtualization environment. It sits between the physical hardware and the virtual machines, allowing multiple VMs to run concurrently. The hypervisor abstracts the underlying hardware and allocates resources to each VM, ensuring isolation and efficient resource utilization.

2. Virtual Machines (VMs): VMs are the virtual instances created within the virtualization environment. Each VM operates as an independent computing system with its own operating system, applications, and resources. VMs provide the ability to run multiple operating systems and applications on a single physical server, enabling efficient resource sharing and flexibility.
3. Virtual Networks: Virtual networks are created within the virtualization environment to enable communication between VMs and with external networks. These virtual networks operate similarly to physical networks, allowing VMs to communicate, share data, and connect to the internet.

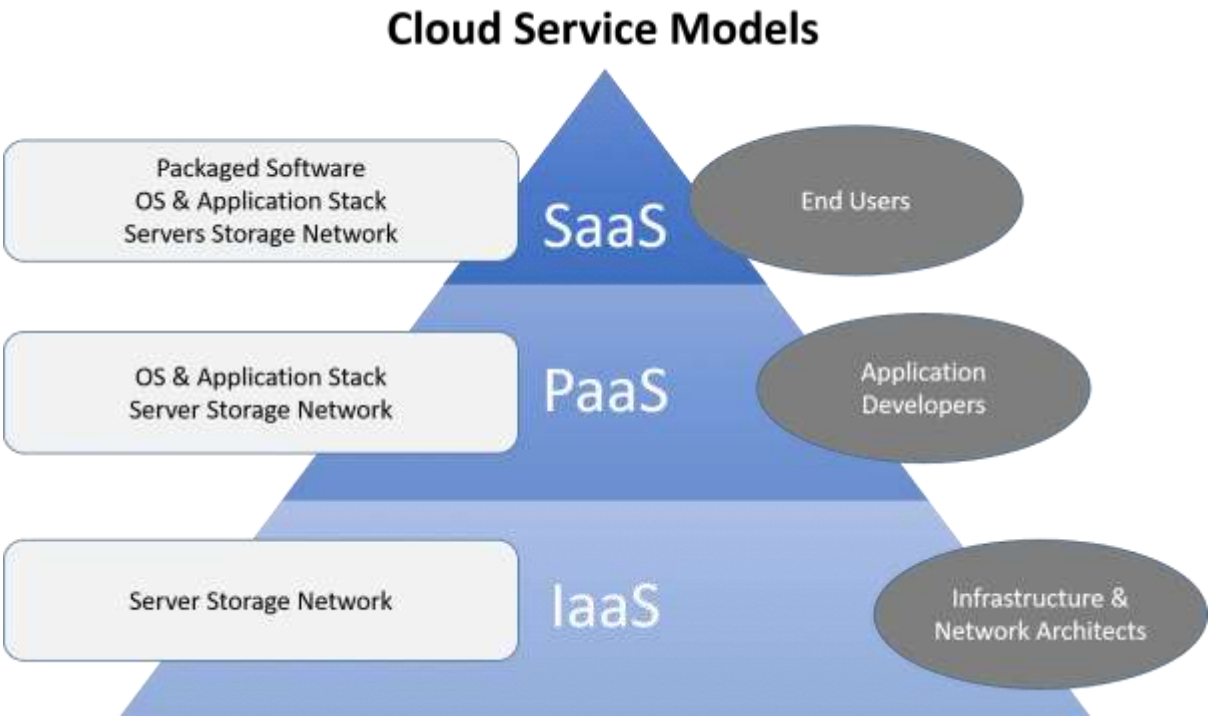
4. Storage Virtualization: Storage virtualization abstracts physical storage devices into virtual storage pools. It allows for the efficient allocation and management of storage resources to

VMs. Storage virtualization provides features such as data redundancy, snapshots, and migration, enhancing data management and resilience.

5. Orchestration and Management Tools: Cloud computing platforms provide orchestration and management tools to control the virtualization environment. These tools enable the provisioning, monitoring, and management of VMs, networks, and storage resources. They offer features like automated scaling, load balancing, and resource optimization to ensure efficient resource utilization.

Types of Cloud Computing based on service models:

Cloud computing offers different service models that cater to varying levels of control and management provided by the cloud provider. The three primary types of cloud computing based on service models are:



1.Infrastructure as a Service (IaaS): IaaS provides users with virtualized computing resources over the internet. Users have control over the operating systems, applications, and storage, while the cloud provider manages the underlying infrastructure, including servers, networking, and data centers. IaaS offers the highest level of flexibility and control, allowing users to build and manage their own virtualized IT infrastructure.

- It is the most flexible type of cloud service which lets you rent the hardware and contains the basic building blocks for cloud and IT.
- It gives complete control over the hardware that runs your application (servers, VMs, storage, networks & operating systems).
- It's an instant computing infrastructure, provisioned and managed over the internet.
- IaaS gives you the very best level of flexibility and management control over your IT resources.
- It is most almost like the prevailing IT resources with which many IT departments and developers are familiar.
- Examples of IaaS: **Virtual machines** or **AWS EC2**, Storage, or Networking.

2.Platform as a Service (PaaS): PaaS provides a platform and environment for users to develop, test, and deploy applications over the internet. Users have control over the applications and data, while the cloud provider manages the underlying infrastructure, including servers, operating systems, and runtime environments. PaaS abstracts the complexities of infrastructure management, allowing developers to focus on application development without worrying about underlying infrastructure details.

- PaaS is a cloud service model that gives a ready-to-use development environment where developers can specialize in writing and executing high-quality code to make customized applications.
- It helps to create an application quickly without managing the underlying infrastructure. For example, when deploying a web application using PaaS, you don't have to install an operating system, web server, or even system updates. However, you can scale and add new features to your services.
- This cloud service model makes the method of developing and deploying applications simpler and it is more expensive than IaaS but less expensive than SaaS.

- This helps you be more efficient as you don't get to worry about resource procurement, capacity planning, software maintenance, patching, or any of the opposite undifferentiated work involved in running your application.
- **Examples** of PaaS: Elastic Beanstalk or Lambda from AWS, WebApps, Functions or Azure SQL DB from Azure, Cloud SQL DB from Google Cloud, or Oracle Database Cloud Service from Oracle Cloud.

3.Software as a Service (SaaS):

SaaS delivers software applications over the internet, allowing users to access and use them on a subscription basis. Users do not have to manage or control the underlying infrastructure, including servers, operating systems, and application runtime. SaaS offers ready-to-use applications that are accessible through web browsers or specific client interfaces. Users can typically customize the application to a certain extent but have limited control over the underlying infrastructure.

- SaaS provides you with a complete product that is run and managed by the service provider.
- The software is hosted online and made available to customers on a subscription basis or for purchase in this cloud service model.
- With a SaaS offering, you don't need to worry about how the service is maintained or how the underlying infrastructure is managed. It would help if you believed how you'd use that specific software.
- **Examples** of SaaS: Microsoft Office 365, Oracle ERP/HCM Cloud, SalesForce, Gmail, or Dropbox.

Cloud Deployment models:

Cloud deployment models refer to different approaches for deploying and accessing cloud computing services. The Three primary Cloud Deployment Models are:

1. **Public Cloud:** In a public cloud deployment, cloud services are provided over the internet by a third-party cloud service provider, such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform. These services are available to the general public or organizations and are typically offered on a pay-as-you-go basis. The infrastructure and resources are shared among multiple customers, offering scalability and cost-efficiency. Public cloud deployments are well-suited for organizations with varying workloads, limited IT resources, or those looking for on-demand scalability.

2. **Private Cloud:** A private cloud deployment involves dedicated cloud infrastructure that is used exclusively by a single organization. The infrastructure can be hosted on-premises within the organization's data center or in a third-party provider's data center. Private clouds provide greater control, security, and customization options, as they are not shared with other organizations. They are often preferred by industries with strict compliance and data security requirements, such as government agencies, financial institutions, and healthcare organizations.

3. **Hybrid Cloud:** Hybrid cloud deployments combine elements of both public and private clouds. They involve integrating and managing resources across multiple cloud environments, including public and private clouds, as well as on-premises infrastructure. This model allows

organizations to leverage the scalability and cost-efficiency of public clouds for non-sensitive workloads, while keeping critical data and applications in a private cloud or on-premises environment. Hybrid clouds provide flexibility, allowing organizations to choose the most suitable deployment option for each workload or application.

Cloud service providers:

There are several major cloud service providers that offer a wide range of cloud computing services and solutions. Here are some of the prominent cloud service providers:

1. **Amazon Web Services (AWS):** AWS, offered by Amazon.com, is one of the largest and most comprehensive cloud platforms. It provides a vast array of services, including computing power (EC2), storage (S3), databases (RDS), networking, analytics, artificial intelligence, machine learning, serverless computing (Lambda), and more. AWS is known for its scalability, global infrastructure, and extensive ecosystem of services.

2. **Microsoft Azure:** Azure, developed by Microsoft, is another leading cloud platform that offers a comprehensive suite of cloud services. It provides services for computing, storage, databases, networking, AI, machine learning, and analytics. Azure also integrates well with Microsoft's other products and services, making it an attractive choice for organizations already using Microsoft technologies.

3. **Google Cloud Platform (GCP):** GCP is Google's cloud computing platform that provides a broad set of cloud services. It offers computing resources, storage, databases, networking, machine learning, data analytics, and IoT (Internet of Things) capabilities. GCP is known for its strong offerings in AI and machine learning, as well as its global infrastructure.

4. **IBM Cloud:** IBM Cloud is IBM's cloud computing platform that provides a wide range of services and solutions. It offers infrastructure services, platform services, software services, and AI-powered services. IBM Cloud is recognized for its focus on enterprise-grade services, including security, compliance, and hybrid cloud deployments.

5. **Oracle Cloud:** Oracle Cloud is Oracle's cloud platform that offers a comprehensive suite of cloud services, including infrastructure, platform, database, analytics, AI, and software services. Oracle Cloud emphasizes its strength in enterprise applications and database management systems.

6. **Alibaba Cloud:** Alibaba Cloud, part of Alibaba Group, is a leading cloud service provider in China and has a growing global presence. It offers a wide range of cloud services, including computing, storage, networking, databases, AI, and analytics. Alibaba Cloud is particularly popular among organizations targeting the Chinese market.

These are just a few examples of major cloud service providers. Each provider offers a unique set of services, pricing models, global regions, and features. When selecting a cloud service provider, organizations consider factors such as their specific requirements, service offerings, performance, scalability, data sovereignty, pricing, support, and integration capabilities.

Introduction to Amazon Web Services:

Amazon Web Services (AWS) is a comprehensive cloud computing platform provided by Amazon.com. It offers a vast array of cloud services that enable individuals and organizations to build and deploy various applications, securely store and manage data, and scale their infrastructure as needed. AWS provides a scalable, reliable, and cost-effective solution for businesses of all sizes, from startups to large enterprises.

AWS offers a wide range of services across numerous categories, including:

1. Compute: AWS Elastic Compute Cloud (EC2) provides virtual servers in the cloud, allowing users to scale compute resources on-demand. EC2 enables organizations to run applications, websites, and backend processes with flexibility and control.

2. Storage: AWS provides multiple storage options. Amazon Simple Storage Service (S3) is a highly scalable object storage service for storing and retrieving data. Amazon Elastic Block Store (EBS) offers persistent block-level storage volumes for EC2 instances. Additionally, AWS provides storage options for archiving (Amazon Glacier), file storage (Amazon Elastic File System), and content delivery (Amazon CloudFront).

3. Databases: AWS offers various database services, including Amazon Relational Database Service (RDS) for managed relational databases, Amazon DynamoDB for fully managed NoSQL databases, and Amazon Aurora for a highly scalable and performant relational database engine. There are also specialized database options for analytics, in-memory caching, and graph databases.

4. Networking: AWS provides networking capabilities such as Amazon Virtual Private Cloud (VPC), which allows users to create isolated virtual networks within the AWS cloud. AWS also offers load balancing, DNS management, content delivery, and virtual private network (VPN) connectivity services.

5. Analytics: AWS offers a range of services for data analytics and processing, including Amazon Redshift for data warehousing, Amazon Athena for interactive query analysis of data stored in S3, and Amazon EMR for big data processing using Apache Hadoop and Spark.

6. AI and Machine Learning: AWS provides services that enable developers to incorporate artificial intelligence and machine learning into their applications. This includes Amazon SageMaker for building, training, and deploying machine learning models, Amazon Rekognition for image and video analysis, and Amazon Lex for building conversational chatbots.

7. Security and Identity: AWS offers numerous services to enhance security and manage access to resources. This includes identity and access management (IAM), security monitoring and logging (Amazon CloudWatch and AWS CloudTrail), encryption services, and dedicated hardware security modules (AWS Key Management Service).

8. Developer Tools: AWS provides a wide range of tools for developers, including AWS CodeStar for managing the entire development lifecycle, AWS CodeCommit for source code version control, AWS CodeBuild for building and testing code, and AWS CodeDeploy for automating application deployments.

These are just a few examples of the many services available on the AWS platform. AWS has a global infrastructure that spans multiple regions worldwide, allowing organizations to deploy their applications and services closer to their target audience for improved performance and latency.

AWS offers flexible pricing models, including pay-as-you-go pricing for most services, along with various pricing tiers and options to optimize costs. The platform also provides extensive documentation, tutorials, and support resources to assist users in getting started and mastering AWS services.

Overall, AWS provides a robust and feature-rich cloud computing platform that enables businesses to leverage the benefits of cloud technology, including scalability, reliability, and cost-efficiency, to drive innovation and achieve their objectives.

Why do Customers move to AWS?

Customers move to AWS (Amazon Web Services) for a variety of reasons. Here are some common motivations for organizations to choose AWS:

1. Scalability and Flexibility: AWS offers a wide range of services and resources that allow customers to scale their infrastructure up or down according to their needs. This flexibility is particularly beneficial for businesses experiencing rapid growth or fluctuating demand.
2. Reliability and Availability: AWS has a global infrastructure that provides high availability and fault tolerance. Customers can leverage AWS's multiple data centers and regions to ensure their applications and data are accessible and protected against failures.
3. Cost Efficiency: AWS operates on a pay-as-you-go model, allowing customers to only pay for the resources they use. This eliminates the need for large upfront investments in hardware and infrastructure, making it cost-effective for businesses of all sizes.
4. Security: AWS provides a wide range of security services and features to help customers protect their data and applications. They offer comprehensive security controls, encryption, and compliance certifications, ensuring that customer data is secure and meets regulatory requirements.
5. Global Footprint: AWS has a vast global infrastructure presence with multiple data centers and regions spread across different continents. This enables customers to deploy their applications and services closer to their target audience, reducing latency and improving performance.
6. Broad Service Portfolio: AWS offers an extensive portfolio of cloud services covering various domains such as compute, storage, databases, machine learning, analytics, IoT, and more. This allows customers to leverage these services to build and deploy a wide range of applications and solutions.
7. Integration and Ecosystem: AWS provides seamless integration with other Amazon services, such as Amazon S3 for storage or Amazon RDS for databases. Additionally, AWS has a thriving ecosystem of third-party providers, tools, and services, allowing customers to enhance their applications and workflows.
8. Innovation and Agility: AWS is known for its continuous innovation and rapid deployment of new services and features. Customers can leverage these advancements to stay ahead of the competition, experiment with new ideas, and quickly bring their products and services to market.
9. Support and Documentation: AWS offers comprehensive documentation, tutorials, and resources to help customers get started and optimize their usage of AWS services. Additionally, AWS provides different levels of support, including enterprise-level support for businesses with specific needs.

These factors contribute to the popularity of AWS and make it an attractive choice for customers looking to migrate their infrastructure to the cloud. However, it's important to note that each organization's specific needs and requirements should be considered when choosing a cloud provider.

Gartner Magic Quadrant for Cloud Infrastructure:

Gartner defines the cloud infrastructure and platform services (CIPS) market as standardized, highly automated offerings, in which infrastructure resources (e.g., compute, networking, and storage) are complemented by integrated platform services. These include managed applications, databases, and functions-as-a-service offerings. The resources are scalable and elastic in near real-time and are metered by use. Self-service interfaces, including a web-based user interface (UI) and an API, are exposed directly to the customer. The resources may be single-tenant or multitenant and can be hosted by a service provider or on-premises in the customer's data center.

The Magic Quadrant assesses cloud infrastructure providers across multiple dimensions, including their product offerings, innovation, market understanding, sales and marketing strategies, customer experience, and overall market presence. The goal is to help organizations make informed decisions when choosing a cloud infrastructure provider.
The Magic Quadrant categorizes providers into four quadrants:
Leaders: These are vendors that have a strong market presence and offer comprehensive cloud infrastructure solutions. They demonstrate a clear vision, innovation, and the ability to execute their strategies effectively. Leaders often have a wide range of services, a strong customer base, and a global presence. **Challengers:** Challengers are vendors that have a solid market presence but may lag behind the Leaders in terms of vision and innovation. They often focus on a specific market segment or have unique strengths in certain areas.
Visionaries: Visionaries are vendors that demonstrate a clear vision and innovation but may have a smaller market presence compared to the Leaders. They often bring unique and differentiated offerings to the market.

Niche Players: Niche Players are vendors that have a limited market presence and may focus on specific niche markets or industries. They may offer specialized solutions or target specific customer segments.
It's important to note that the Gartner Magic Quadrant is just one of many resources that organizations can consider when evaluating cloud infrastructure providers. It's recommended to review multiple sources of information, including analyst reports, customer reviews, and your specific business requirements, to make an informed decision.

AWS Global Infrastructure:

The AWS Global Cloud Infrastructure is the most secure, extensive, and reliable cloud platform, offering over 200 fully featured services from data centres globally. Whether you need to deploy your application workloads across the globe in a single click, or you want to build and deploy specific applications closer to your end-users with single-digit millisecond latency, AWS provides you the cloud infrastructure where and when you need it. With millions of active customers and tens of thousands of partners globally, AWS has the largest and most dynamic ecosystem. Customers across virtually every industry and of every size, including start-ups, enterprises, and public sector organizations, are running every imaginable use case on AWS.
Here are some key components of AWS's global infrastructure:

Regions: AWS operates in multiple geographic regions across the globe. Each region consists of multiple data centers, referred to as Availability Zones (AZs), that are isolated from each other in terms of power, cooling, and network connectivity. As of my knowledge cutoff in September 2021, AWS had 25 regions globally, including the Americas, Europe, Asia Pacific, and the Middle East.

Availability Zones (AZs): Availability Zones are physically separate data centers within a region. They are designed to be isolated from each other to provide fault tolerance and high availability. Each AZ typically has its own power infrastructure, networking, and cooling systems. AWS recommends deploying applications across multiple AZs to achieve resilience and minimize downtime.

Edge Locations: In addition to regions and AZs, AWS has a network of edge locations. These edge locations serve as content delivery endpoints for AWS's content delivery network (CDN) service called Amazon CloudFront. Edge locations are distributed across many cities globally and help improve the performance of content delivery by bringing it closer to end users.

Global Network: AWS has built a global network infrastructure that connects its regions, AZs, and edge locations. This network includes high-speed private links, redundant connections, and optimized routing to ensure low-latency and high-bandwidth connectivity between different parts of the AWS infrastructure.

Services: AWS provides a vast portfolio of cloud services and solutions that can be deployed globally. These services include computing, storage, networking, databases, machine learning, analytics, IoT, security, and more. Customers can choose to deploy their applications and data in multiple regions or AZs to achieve global coverage and redundancy.

It's worth noting that AWS continues to expand and add new regions and services to its infrastructure over time. For the most up-to-date and detailed information, I recommend visiting the official AWS website or consulting AWS documentation.

What to Consider when Selecting a Region for your Workloads

When selecting a region for your workloads in AWS (Amazon Web Services), it's important to consider several factors related to the AWS global infrastructure. Here are some key considerations:

1.Proximity to Users: Choose a region that is geographically close to your target audience or users. This helps reduce network latency and provides better performance for your applications and services. Lower latency can result in improved user experience and faster response times.

2.Availability of Services: Not all AWS services are available in every region. Review the AWS Regional Services List to ensure that the required services for your workloads are available in your chosen region. Consider whether the region offers the specific services and features you need to build and deploy your applications.

3.Availability Zone (AZ) Distribution: AWS regions are divided into multiple Availability Zones (AZs), which are physically separate data centers within the region. Check the number of AZs available in a region and consider deploying

your workloads across multiple AZs for high availability and fault tolerance. Distributing your resources across AZs helps protect your applications from single points of failure.

4.Compliance and Data Residency: Different regions may have varying compliance requirements and regulations. Consider the specific compliance needs of your industry or organization and ensure that the chosen region complies with those requirements. Also, take into account data residency concerns if there are restrictions on where your data can be stored.

5.Data Transfer Costs: AWS charges for data transfer between regions or Availability Zones. If you have workloads that require frequent data replication or transfer between regions, consider the potential impact on data transfer costs.

6.Disaster Recovery and Business Continuity: Selecting a region for disaster recovery purposes involves choosing a region that is geographically separate from your primary region. This ensures that in the event of a regional outage or disaster, your workloads and data can be quickly restored in the alternate region.

7.Pricing: Pricing for AWS services can vary by region. Take into account the pricing differences for the services you plan to use in different regions. Evaluate the cost implications of running your workloads in different regions to align with your budget and cost considerations.

8.Support and Service Level Agreements (SLAs): Check the support options and SLAs available for the chosen region. Ensure that the support levels and SLAs meet your business requirements and align with your expected response times and availability needs.

9.Regulatory and Legal Considerations: Consider any specific legal and regulatory requirements that may apply to your workloads. This includes data privacy laws, industry-specific regulations, and government restrictions. Ensure that the chosen region complies with the necessary regulations and legal obligations.

10.Local Infrastructure and Connectivity: Evaluate the availability and quality of local infrastructure and connectivity in the chosen region. Consider factors such as power availability, network connectivity, and access to other necessary resources.

By considering these factors, you can make an informed decision when selecting the AWS region that best suits your specific requirements for performance, compliance, cost, and disaster recovery. AWS provides detailed documentation and resources to help you understand the capabilities and considerations of each region, enabling you to choose the optimal region for your workloads.

Shared responsibility model

The shared responsibility model is a framework that defines the security responsibilities and division of tasks between cloud service providers (CSPs) like AWS (Amazon Web Services) and their customers. It helps clarify which security aspects are managed by the CSP and which are the responsibility of the customer. In the context of AWS, the shared responsibility model can be summarized as follows:

AWS Responsibility:

Security of the cloud: AWS is responsible for securing the underlying infrastructure, data centers, and global network that AWS services operate on.

Managed services: AWS is responsible for the security and compliance of its managed services, such as Amazon RDS, Amazon S3, and AWS Lambda.

Customer Responsibility:
Security in the cloud: Customers are responsible for the security of their applications, data, and operating systems running on AWS. This includes implementing appropriate access controls, securing network configurations, and protecting against security threats.

Compliance and data privacy: Customers are responsible for complying with applicable regulations and protecting the privacy and confidentiality of their data. Identity and access management (IAM): Customers are responsible for managing user access and IAM policies for their AWS accounts, as well as controlling access to their AWS resources.

Configuration management: Customers are responsible for configuring and securing their AWS resources, including virtual machines, storage, and databases.
Data protection: Customers are responsible for implementing data encryption, both in transit and at rest, and managing encryption keys.

Patch management: Customers are responsible for applying patches and updates to their operating systems and applications running on AWS.

It's important to note that while AWS provides a secure and compliant infrastructure, following security best practices and implementing appropriate controls are essential to fully secure the customer's workloads and data on AWS.
Understanding the shared responsibility model is crucial for customers to ensure they meet their security obligations and make informed decisions regarding security configurations and practices on the AWS platform. AWS provides extensive documentation, security-related services, and best practice guides to assist customers in fulfilling their responsibilities within the shared responsibility model.

AWS Documentation:

The AWS (Amazon Web Services) Documentation is a comprehensive resource that provides detailed information, guides, tutorials, and reference materials for using and understanding AWS services. It serves as a valuable reference for developers, architects, system administrators, and anyone working with AWS. The AWS Documentation covers a wide range of topics, including:

1.Service Guides: Each AWS service has its dedicated documentation, providing an overview of the service, its features, and how to use it. These guides include detailed instructions, code examples, best practices, and use cases specific to each service.

2.Developer Guides: AWS offers developer guides that focus on various programming languages and development platforms. These guides provide SDK (Software Development Kit) documentation, API references, sample code, and step-by-step instructions for integrating AWS services into your applications.

3.Architecture Center: The AWS Architecture Center provides guidance and best practices for designing and implementing solutions on AWS. It includes reference architectures, whitepapers, and design patterns to help you architect secure, scalable, and cost-effective systems on the AWS cloud.

4.SDK and API References: AWS provides comprehensive documentation for its SDKs and APIs, allowing developers to interact with AWS services programmatically. These references include information on classes, methods, parameters, and response structures, helping developers integrate AWS services into their applications.

5.AWS CLI (Command Line Interface) Documentation: The AWS CLI documentation offers guidance on using the AWS CLI tool to interact with AWS services from the command line. It provides commands, options, and usage examples for various AWS operations.

6.AWS Well-Architected Framework: The AWS Well-Architected Framework documentation provides guidance on building and operating reliable, secure, efficient, and cost-effective systems in the AWS cloud. It offers best practices, design principles, and assessment tools to help you evaluate and improve the architecture of your applications.

7.Security and Compliance Documentation: AWS places a strong emphasis on security and compliance. The AWS documentation provides detailed information on AWS security features, identity and access management, encryption, network security, and compliance with various industry standards and regulations.

AWS Support Plans:

AWS (Amazon Web Services) offers different support plans to cater to varying customer needs. Here are the main AWS support plans available:

1.Basic Support: Basic Support is available to all AWS customers at no additional cost. It includes access to AWS documentation, forums, and whitepapers. Basic Support also provides access to the AWS Trusted Advisor service, which offers recommendations to help optimize your AWS infrastructure, enhance security, and improve performance.

2.Developer Support: Developer Support is designed for developers and organizations getting started with AWS. It includes all the features of Basic Support and adds several benefits, such as email-based support for technical questions and guidance from AWS experts, with a response time within 24 business hours.

3.Business Support: Business Support is suitable for production workloads and businesses requiring faster response times and more comprehensive support. It includes all the features of Developer Support and provides access to AWS Support via phone, chat, and email 24/7. Business Support also offers assistance with architectural and operational best practices, guidance for AWS services, and assistance with service-related incidents.

4.Enterprise Support: Enterprise Support is the highest level of support offered by AWS and is designed for businesses with mission-critical workloads and complex environments. It includes all the features of Business Support and adds several premium benefits. These include a designated Technical Account Manager (TAM) who serves as a single point of contact, assistance with architectural reviews and operational reviews, and support for high-priority and business-critical incidents.

Each support plan has different pricing tiers based on your monthly usage and the level of support required. The pricing varies depending on the AWS services you use, the region, and the support plan you select.
It's important to note that AWS Support plans are separate from the technical support provided by AWS Marketplace sellers. If you are using third-party software or services from the AWS Marketplace, you may need to consult the seller's support options and plans.

Billing Dashboard:

The AWS Billing Dashboard is a web-based interface within the AWS Management Console that provides comprehensive information and tools for managing your AWS billing and cost management.

1.Cost Explorer: The Cost Explorer is a tool within the Billing Dashboard that allows you to analyze and visualize your AWS costs and usage over time. It
provides charts, graphs, and reports to help you understand your spending patterns, identify cost drivers, and optimize your resource allocation.

2.Cost and Usage Reports: The Billing Dashboard allows you to generate and download detailed cost and usage reports in CSV or Parquet format. These reports provide granular information about your AWS usage, resource costs, and usage trends, allowing you to perform more in-depth analysis and cost allocation.

3.Budgets and Cost Alerts: You can set up budgets within the Billing Dashboard to define spending thresholds and receive notifications when your costs exceed the defined limits. This helps you proactively monitor and control your AWS spending to avoid unexpected charges.

4.Payment Methods and Invoices: The Billing Dashboard provides options for managing your payment methods, such as credit cards or bank accounts, and allows you to view and download invoices for your AWS charges.

5.Linked Accounts and Consolidated Billing: If you have multiple AWS accounts, the Billing Dashboard enables you to set up consolidated billing, which allows you to view and manage the billing and cost information for all linked accounts in a single dashboard. This makes it easier to track and manage costs across multiple AWS accounts.

6.Cost Allocation Tags: The Billing Dashboard supports cost allocation tags, which allow you to assign custom metadata to your AWS resources. This enables you to categorize and track costs by specific attributes, such as departments, projects, or applications, making it easier to allocate and analyze costs based on your organizational structure.

7.AWS Marketplace Subscriptions: If you subscribe to AWS Marketplace products or services, the Billing Dashboard provides a consolidated view of your subscriptions, allowing you to manage and monitor your AWS Marketplace usage and costs.

The AWS Billing Dashboard provides a centralized and user-friendly interface for managing and understanding your AWS billing and cost information. It helps you gain insights into your spending, optimize resource usage, and maintain control over your AWS costs.

Ways to access the AWS Cloud Platform:

There are several ways to access the AWS (Amazon Web Services) cloud platform, depending on your needs and preferences. Here are some common methods:

1.AWS Management Console: The AWS Management Console is a web-based interface that allows you to access and manage your AWS resources. It provides a graphical user interface (GUI) with a comprehensive set of tools for managing various services, configuring settings, and monitoring your infrastructure.

2.AWS Command Line Interface (CLI): The AWS CLI is a command-line tool that enables you to interact with AWS services using commands in a terminal or command prompt. It provides a powerful and scriptable interface for automating tasks, managing resources, and integrating with other tools and systems.

3.AWS Software Development Kits (SDKs): AWS provides SDKs for several programming languages, including Python, Java, .NET, Ruby, and more.
These SDKs allow you to interact with AWS services programmatically, enabling you to build applications, manage resources, and automate workflows.

4.AWS Tools for PowerShell: If you prefer using PowerShell, AWS offers the AWS Tools for PowerShell, which provides a set of cmdlets for managing and interacting with AWS services from the PowerShell command-line interface.

5.AWS APIs and SDKs: AWS provides a comprehensive set of APIs (Application Programming Interfaces) that allow you to integrate AWS services into your own applications or systems. These APIs enable programmatic access to AWS resources and services, giving you full control and flexibility.

6.AWS Mobile App: AWS offers a mobile app for iOS and Android devices that provides a simplified view of your AWS resources, allowing you to monitor and manage your infrastructure on the go.

7.Third-Party Tools and Integrations: There are also various third-party tools and integrations available that provide additional ways to access and interact with the AWS cloud platform. These tools may offer specialized functionalities, enhanced monitoring capabilities, or specific integrations with other systems or services.

AWS FREE TIER:

The AWS Free Tier is a program offered by Amazon Web Services that provides customers with limited access to several AWS services at no cost. It allows users to explore and experiment with AWS services without incurring charges, making it a great starting point for individuals and businesses looking to get hands-on experience with AWS.
The AWS Free Tier consists of three different types of offers:

Always Free: This category includes certain services that are available for free on an ongoing basis, even beyond the first 12 months of account creation. Some examples of services in the Always Free tier include AWS Lambda (one million free requests per month), Amazon S3 (5 GB of storage, 20,000 GETrequests, and 2,000 PUT requests per month), and Amazon CloudWatch (10 custom metrics and 10 alarms).

12 Months Free: For the first 12 months after creating an AWS account, eligible services are provided with specific usage limits for free. These limits vary depending on the service and are designed to allow users to get started with AWS. Popular services that are included in the 12 Months Free tier are Amazon EC2 (750 hours of Linux or Windows t2.micro instances per month), Amazon RDS (750 hours of db.t2.micro instances for Amazon RDS for MySQL, PostgreSQL, or MariaDB), and Amazon DynamoDB (25 GB of
storage and 25 read/write capacity units per month).

Trial Offers: AWS also provides trial offers for certain services that are free for a limited period beyond the first 12 months. These trial offers allow users to explore additional AWS services and features. Examples of services with trial offers include Amazon Connect (90 minutes of Amazon Connect usage per month for 12 months) and AWS Glue (one million AWS Glue Data Catalog objects stored for 12 months).

It's important to note that while many services are available under the AWS Free Tier, there are usage limits associated with each service. Once you exceed these limits or start using services not covered by the Free Tier, you will be billed at the regular AWS pricing rates.
To get started with the AWS Free Tier, you can sign up for an AWS account and review the documentation provided by AWS to understand the eligible services, usage limits, and any additional requirements or restrictions.

Total Cost of Ownership(TCO):

Total Cost of Ownership (TCO) analysis is also relevant when considering the adoption of AWS (Amazon Web Services) cloud services. AWS provides a wide range of services that can be utilized to build and operate applications, store and process data, and manage infrastructure.

When calculating TCO in the context of AWS, the following factors should be taken into account:

- Compute and Storage Costs: AWS offers various compute options, such as EC2 instances, which have different pricing models based on instance types, usage, and duration. Storage costs include Amazon S3 (Simple Storage Service), EBS (Elastic Block Store), and Glacier for long-term storage. TCO analysis should consider the projected usage and data storage requirements to estimate these costs accurately.

- Network and Load Balancer Costs: If your application requires network bandwidth or load balancing, AWS offers services like Amazon VPC (Virtual Private Cloud) and Elastic Load Balancer. TCO analysis should account for the associated costs based on your networking requirements.

- Database Costs: AWS provides managed database services like Amazon RDS (Relational Database Service) and Amazon DynamoDB. TCO analysis should consider the chosen database service, storage requirements, and the anticipated number of read/write operations to estimate the associated costs.

- Management and Support Costs: AWS offers various management and support services, such as AWS Management Console, AWS Identity and Access Management (IAM), and AWS Support plans. TCO analysis should include the costs associated with managing and supporting your AWS resources.

- Additional Services and Tools: Depending on your specific requirements, you may need to consider the costs of additional AWS services and tools, such as AWS Lambda (serverless computing), AWS CloudFront (content delivery network), AWS Elastic Beanstalk (application deployment platform), or AWS CloudWatch (monitoring and logging).

In addition to the direct costs of utilizing AWS services, TCO analysis should also consider factors like application development and maintenance costs, employee training and expertise, potential savings from scaling infrastructure, and the impact on business agility and innovation.

Available AWS Certifications:

Importance of AWS IAM:

1.Security: IAM enables you to manage access to your AWS resources securely. By creating IAM users and assigning them appropriate permissions, you can ensure that only authorized individuals or services can access and interact with your AWS resources. IAM helps implement the principle of least privilege, granting users only the necessary permissions to perform their tasks, thereby reducing the risk of unauthorized access, data breaches, and malicious activities.

2.Granular Access Control: IAM allows you to define fine-grained permissions for your users, groups, and roles. You can precisely specify which AWS services, APIs, actions, and resources each user can access and what operations they can perform. This level of control helps enforce security best practices and limits the potential impact of any compromised credentials.

3.Centralized User Management: With IAM, you can centrally manage user accounts, groups, and roles within your AWS account. This makes it easier to provision and deprovision access for individuals joining or leaving your organization. IAM supports various user management capabilities, such as password policies, multi-factor authentication (MFA), and integration with external identity providers, enabling seamless and secure user authentication and access control.

4.Auditing and Compliance: IAM provides detailed logs and monitoring capabilities, allowing you to track and audit user activity within your AWS environment. You can gain insights into who accessed what resources, when, and from where. These logs are valuable for security analysis, troubleshooting, and meeting regulatory compliance requirements.

AWS Root User Vs IAM User

The AWS (Amazon Web Services) root user and IAM (Identity and Access Management) user are two different types of accounts with different levels of permissions and responsibilities within an AWS environment.

1.Root User:

- The root user is created automatically when you sign up for an AWS account.
- It has full administrative privileges and unrestricted access to all AWS resources and services.
- The root user has the highest level of permissions and should be used sparingly for security reasons.
- It is recommended to create and use IAM users with appropriate permissions instead of relying on the root user for day-to-day operations.
- The root user account is typically used for initial setup, billing, and critical account management tasks.

2.IAM User:

- IAM allows you to create multiple users within your AWS account with specific permissions and roles.
- IAM users are separate from the root user and have their own credentials and access keys.
- IAM users are assigned individual permissions based on the principle of least privilege, meaning they only have access to the resources and services required for their specific tasks.
- IAM users can be granted or denied access to different AWS services, APIs, and resources.
- IAM allows for the central management of user accounts, including password policies, multi-factor authentication (MFA), and access keys.
- IAM users can be grouped into IAM groups and assigned policies to manage access collectively.

AWS Elastic Compute Cloud(EC2):

What is EC2 in AWS?

The full form of Amazon EC2 is Amazon Elastic Compute Cloud. Amazon EC2 is one of the most used and most basic services on Amazon so it makes sense to start with EC2 when you are new to AWS.

Well, to be very simple, EC2 is a machine with an operating system and hardware components of your choice. But the difference is that it is totally virtualized. You can run multiple virtual computers in a single physical hardware.

Elastic Compute Cloud (EC2) is one of the integral parts of the AWS ecosystem. EC2 enables on-demand, scalable computing capacity in the AWS cloud.

Amazon EC2 instances eliminate the up-front investment for hardware, and there is no need to maintain any rented hardware. It enables you to build and run applications faster. You can use EC2 in AWS to launch as many virtual servers as you need. Also, you can scale up or down when there is an increase or decrease in website traffic.

The word ‘elastic’ in Elastic Compute Cloud talks about the system’s capability of adapting to varying workloads and provisioning or de-provisioning resources according to the demand.

Why Amazon EC2?

Now that we know the EC2 overview, let’s now move forward and understand Why exactly we need Amazon EC2. AWS Elastic Compute Cloud provides a lot of benefits, let me give you an overview of what I am going to discuss.

- Auto-scaling
- Pay-as-you-go
- Increased Reliability
- Elasticity

Auto-scaling:

This is the benefit that makes most businesses opt for AWS EC2. It is already explained earlier how Netflix uses Amazon EC2 auto-scaling to its advantage and provides a crash-free experience.

Auto-scaling is basically providing resources according to the demand. They either scale up or scale down corresponding to the increase or decrease in demand.

Pay-as-you-go:

You will be charged by the hour, and you have to pay only for what you have used. A company, XYZ might be using 100 servers normally, and on Mondays, it scales down to 50 servers. So, it only has to pay for 50 servers those days, not the usual fee for the usage of 100 servers.

Even when you use your Amazon EC2 instances services for a few hours, you only need to pay for that time period and nothing more.

Increased Reliability:

AWS is spread across 20 worldwide regions with 61 availability zones (AZs) which helps your business when it is expanding. Also, this will increase the load speed of your application around the world.

You can always store multiple copies of your application in multiple AZs so that when one data center fails or loses data, the application will not fail completely.

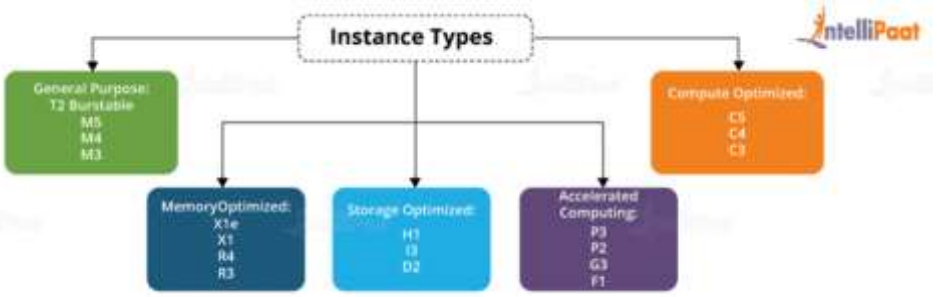
Elasticity:

Instead of 10 low-configuration machines, you could rent a single high-configuration machine with an OS of your preferred choice for your application. Elasticity is the feature from which Elastic Compute Cloud got its name.

Moving on, let's now see different types of Amazon EC2 Instance Types.

AWS EC2 Instance Types

AWS EC2 instance types determine the underlying hardware of the instances which are launched.



There are several types of AWS instances with different configurations and benefits.

- General purpose
- Compute optimized
- Memory-optimized
- Accelerated Computing
- Storage optimized

AWS Simple Storage Service(S3):

Amazon S3 (Simple Storage Service) provides object storage, which is built for storing and recovering any amount of information or data from anywhere over the internet. It provides this storage through a web services interface. While designed for developers for easier web-scale computing, it provides 99.999999999 percent durability and 99.99 percent availability of objects. It can also store computer files up to 5 terabytes in size.

AWS S3 Benefits:

Some of the benefits of AWS S3 are:

- Durability: S3 provides 99.999999999 percent durability.

- Low cost: S3 lets you store data in a range of "storage classes." These classes are based on the frequency and immediacy you require in accessing files. Scalability: S3 charges you only for what resources you actually use, and there are no hidden fees or overage charges. You can scale your storage resources to easily meet your organization's ever-changing demands.

- Availability: S3 offers 99.99 percent availability of objects
- Security: S3 offers an impressive range of access management tools and encryption features that provide top-notch security.
- Flexibility: S3 is ideal for a wide range of uses like data storage, data backup, software delivery, data archiving, disaster recovery, website hosting, mobile applications, IoT devices, and much more.
- Simple data transfer: You don't have to be an IT genius to execute data transfers on S3. The service revolves around simplicity and ease of use.

These are compelling reasons to sign up for S3. Now, let's move on and have a look at some of the major components of the AWS S3 storage service.

Amazon S3 concepts:
Buckets

- To upload your data (photos, videos, documents etc.) to Amazon S3, you must first create an S3 bucket in one of the AWS Regions.
- A bucket is a region specific
- A bucket is a container for objects stored in Amazon S3.
- Every object is contained in a bucket.
- By default, you can create up to 100 buckets in each of your AWS accounts. If you need more buckets,you can increase your account bucket limit to a maximum of 1,000 buckets by submitting a servicelimit increase.
- For example, if the object named photos/puppy.jpg is stored in the john bucket in the US West (Oregon) Region, then it is addressable using the URL https://john.s3.us-west-2.amazonaws.com/photos/puppy.jpg

Region

- You can choose the geographical AWS Region where Amazon S3 will store the buckets that you create.

- You might choose a Region to optimize latency, minimize costs, or address regulatory requirements.
- Objects stored in a Region never leave the Region unless you explicitly transfer them to another Region.
- For example, objects stored in the Europe (Ireland) Region never leave it.

Object

- Amazon S3 is a simple key, value store designed to store as many objects as you want.
- You store these objects in one or more buckets.
- S3 supports object level storage i.e., it stores the file as a whole and does not divide them
- An object size can be in between 0 KB and 5 TB
- When you upload an object in a bucket, it replicates itself in multiple availability zones in the same Region

An object consists of the following:

- Key – The name that you assign to an object.
- Version ID – Within a bucket, a key and version ID uniquely identify an object.
- Value – The content that you are storing.
- Metadata – A set of name-value pairs with which you can store information regarding the object.

AWS Identity and Access Management (IAM):

With AWS Identity and Access Management (IAM), you can specify who or what can access services andresources in AWS, centrally manage fine-grained permissions, and analyze access to refine permissions
across AWS

Features of IAM

- Shared access to your AWS account
- Granular permissions
- Secure access to AWS resources for applications that run on Amazon EC2
- Multi-factor authentication (MFA)
- Integrated with many AWS services
- Eventually Consistent
- IAM achieves high availability by replicating data across multiple servers within Amazon's data centers around the world
- Free to use

IAM Users

- For greater security and organization, you can give accessto your AWS account to specific users—identities that youcreate with custom permissions
- Instead of sharing your root user credentials with others,you can create individual IAM users within your account that correspond to users in your organization
- IAM users are not separate accounts, they are userswithin your account
- Each user can have its own password for access to theAWS Management Console

IAM User Groups

- An IAM group is a collection of IAM users

- You can use groups to specify permissionsfor a collection of users, which can makethose permissions easier to manage forthose users
- For example, you could have a group called Admins and give that groupthe types of permissions that administrators typically need
- Any user in that group automaticallyhas the permissions that are assignedto the group
- It is only a way to attach policies tomultiple users at one time

IAM Roles

- An IAM role is an IAM identity that you can create in your account that has specific permissions
- An IAM role is similar to an IAM user, in that it is anAWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated withone person, a role is intended to be assumable by anyone who needs it
- You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources
- For example, you might want to grant users in your AWS account access to resources they don't usually have, or grant users in one AWS account access to resources in another account

IAM Policies

- You manage access in AWS by creating policies and attaching them to IAM identities (users, groups of users, or roles) or AWS resources
- A policy is an object in AWS that,when associated with an identity or resource, defines their permissions
- AWS evaluates these policies when an IAM principal (user or role) makes a request
- Permissions in the policies determine whether the request is allowed or denied
- Most policies are stored in AWS as JSON documents

Access keys and Secret keys

− Access keys are long-term credentials for an IAM user or the AWS account root user
− Can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK)
− Access keys consist of two parts
− An access key ID (for example, AKIAIOSFODNN7EXAMPLE)
− A Secret access key (for example, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY)

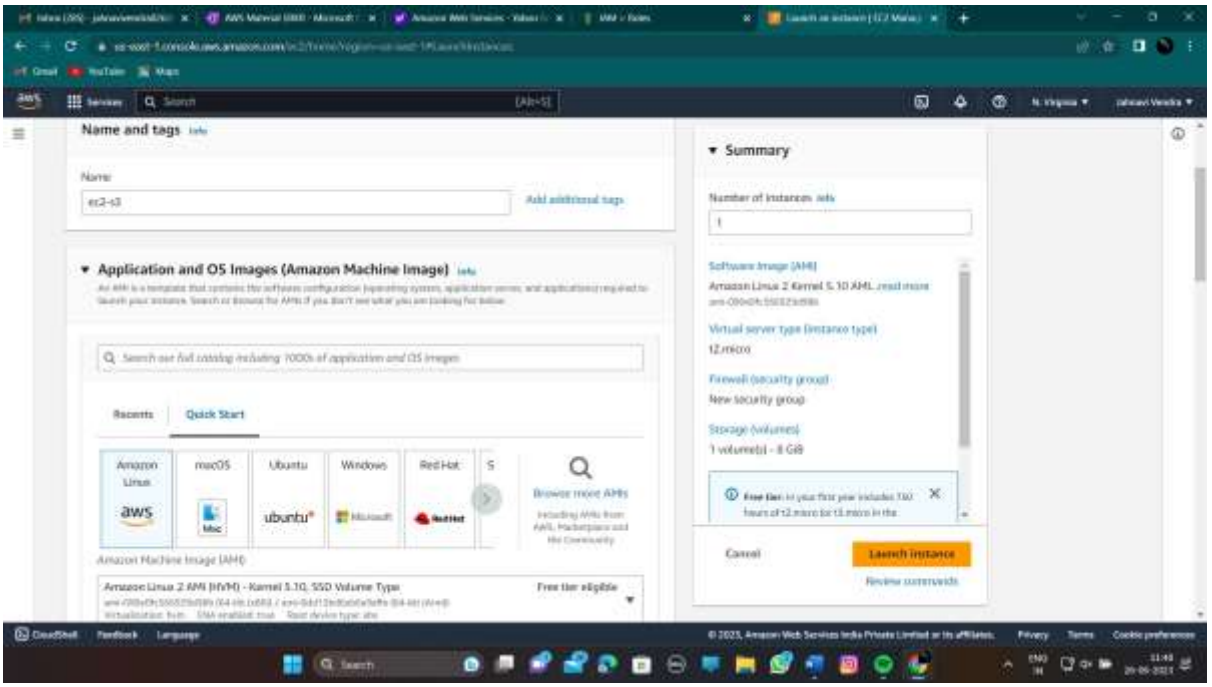
Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests

.

Execution steps:

1. **Launch an EC2 instance with Amazon Linux as AMI.**

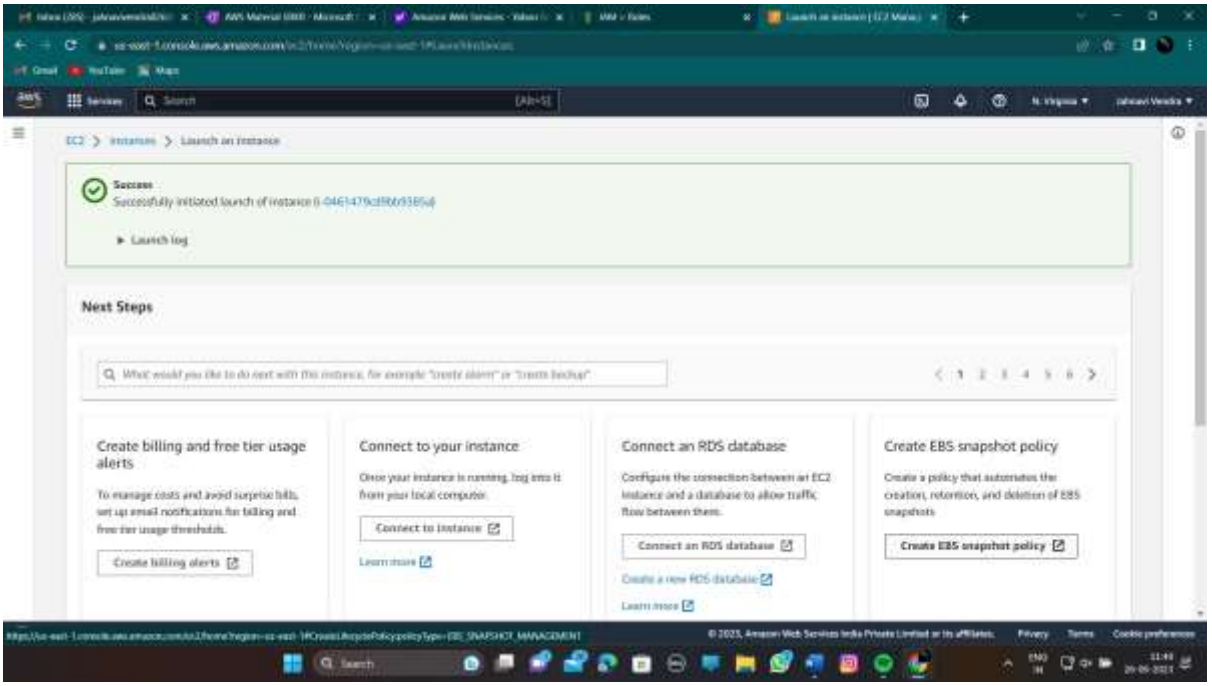
- Open the AWS console and navigate to the EC2 service.
- In the EC2 Dashboard, locate and click on the "Launch instance" button.
- In the instance launch wizard, specify a name for your instance.
- From the available options, choose an Amazon Machine Image (AMI) such as "Amazon Linux" that is eligible for the free tier.
- Select the desired instance type. Select the free tier, you can choose the t2.micro instance type.
- If you have a pre-existing key pair, select it. Otherwise, create a new key pair for secure access to your instance.
- The is key pair is in the format of .pem file



To configure network settings and launch the EC2 instance, follow these additional steps:

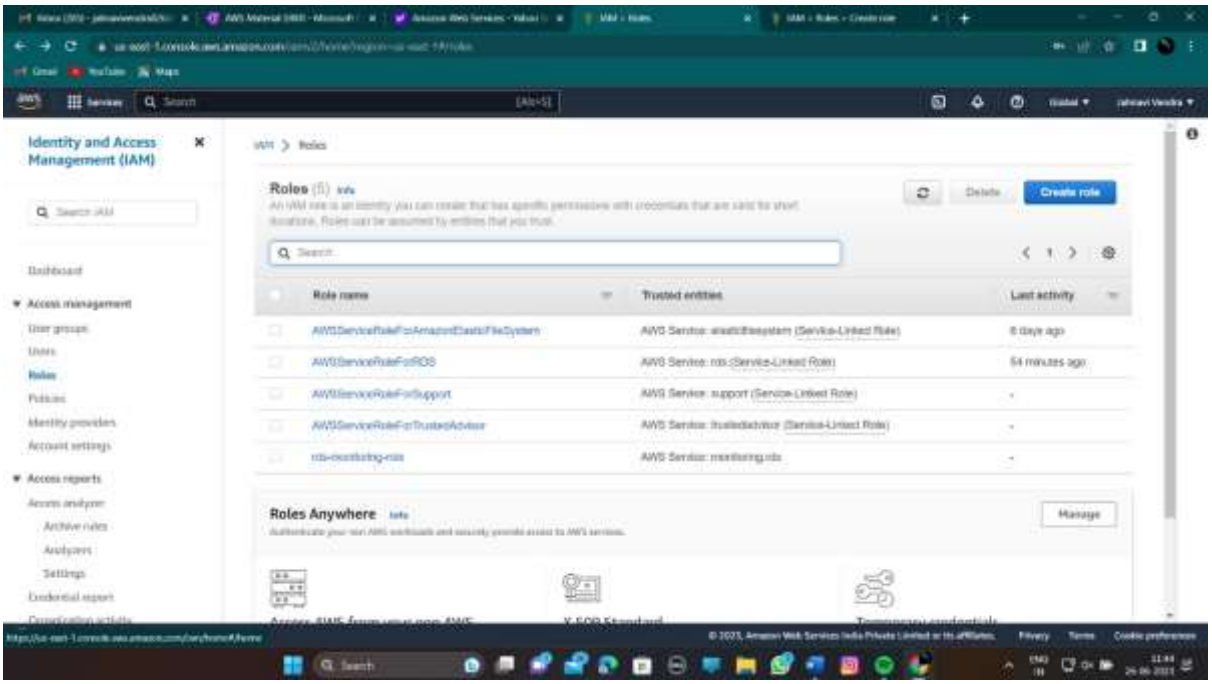
- In the instance launch wizard, navigate to the "Network settings" section and click on the "Edit" option.
- Choose the default Virtual Private Cloud (VPC) for your instance.
- From the list of subnets in the available availability zones, select a subnet in a zone such as "us-east-1a".
- Under the "Security groups" section, you can either select an existing security group or create a new one.
- Ensure that the inbound security group rule type is set to "SSH" and the source type is set to "Anywhere". This allows SSH access to your instance from any source.
- In the "Configure storage" section, specify the desired storage space. For the free tier, you can allocate up to 30GB of storage.
- Leave the remaining settings as default or configure them according to your requirements.
- Finally, click on the "Launch instance" button to initiate the instance launch process.
- Once launched, your instance will be created successfully.

- You can view the instance is created sucessfully

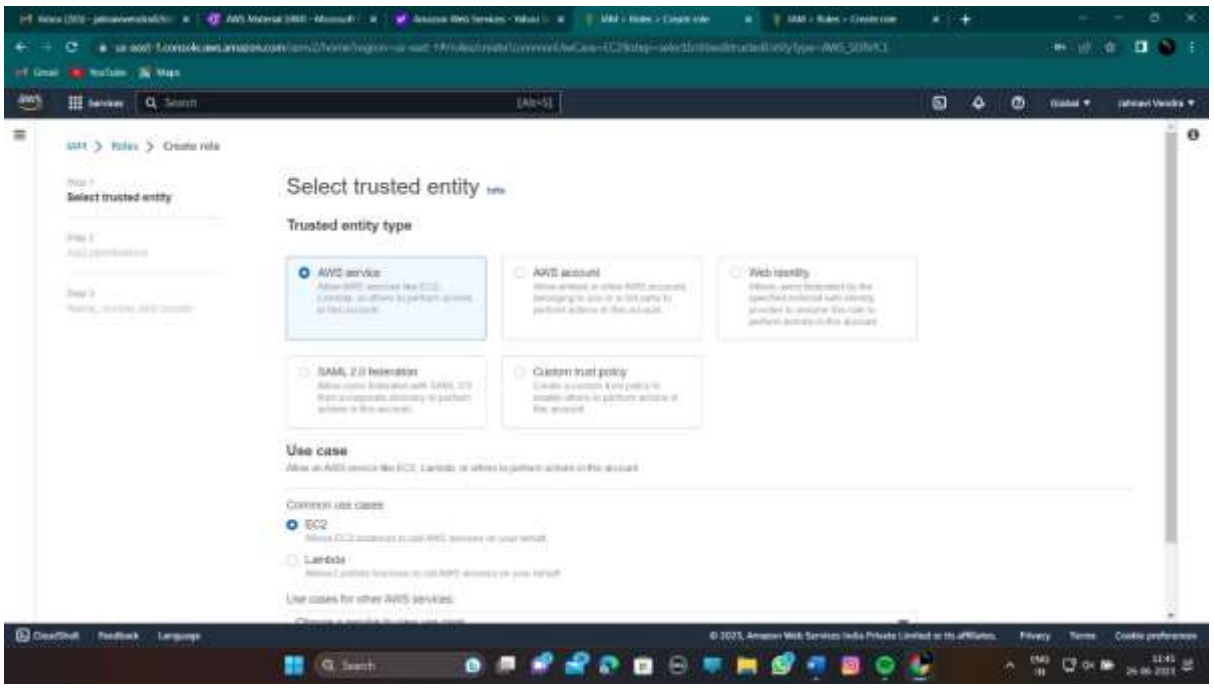


2. Create an IAM Role for EC2 with S3 full access policy and assign to EC2

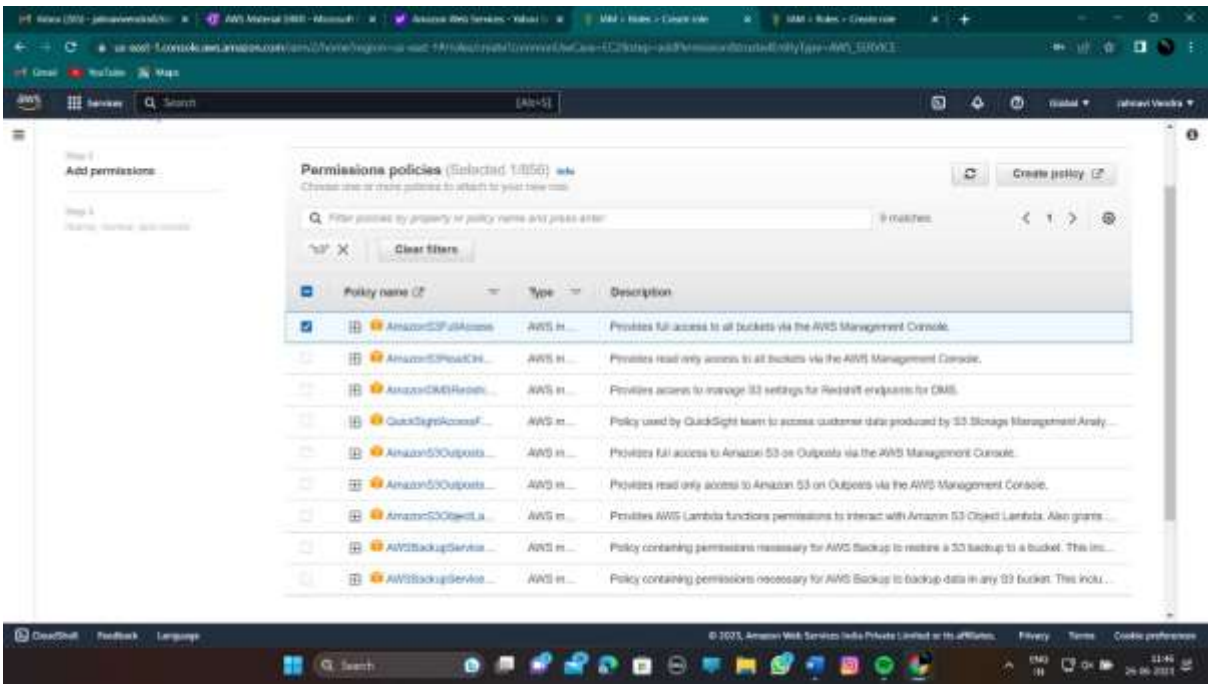
- To create an IAM role for EC2 with the S3 full access policy and assign it to an EC2 instance, follow these steps:
- Go to the IAM (Identity and Access Management) console by signing in to the AWS Management Console and selecting IAM from the services.
- In the IAM console, click on "Roles" in the left sidebar.
- Click on the "Create role" button to start creating a new role.
- On the "Create role" page, select the "AWS service" as the trusted entity.
- Choose "EC2" from the list of services that will use this role and click on the "Next: Permissions" button.



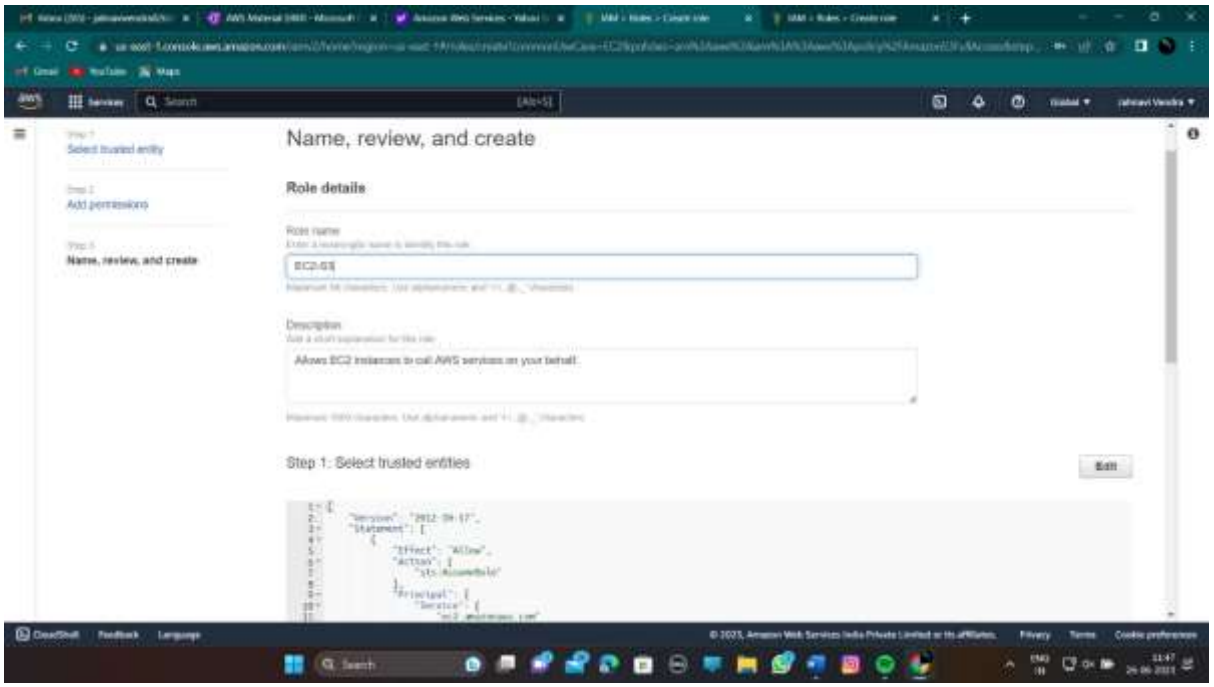
- In the "Attach permissions policies" step, search for the "AmazonS3FullAccess" policy by typing it in the search box.
- Select the policy by clicking the checkbox next to it.
- Click on the "Next: Tags" button to proceed to the next step (you can add tags if needed).
- Click on the "Next: Review" button to review the role details.
- Provide a name for the role in the "Role name" field, such as "EC2-S3-FullAccess-Role".
- Optionally, you can provide a description for the role.
- Review the role details and make sure the S3 full access policy is attached.
- Click on the "Create role" button to create the role.



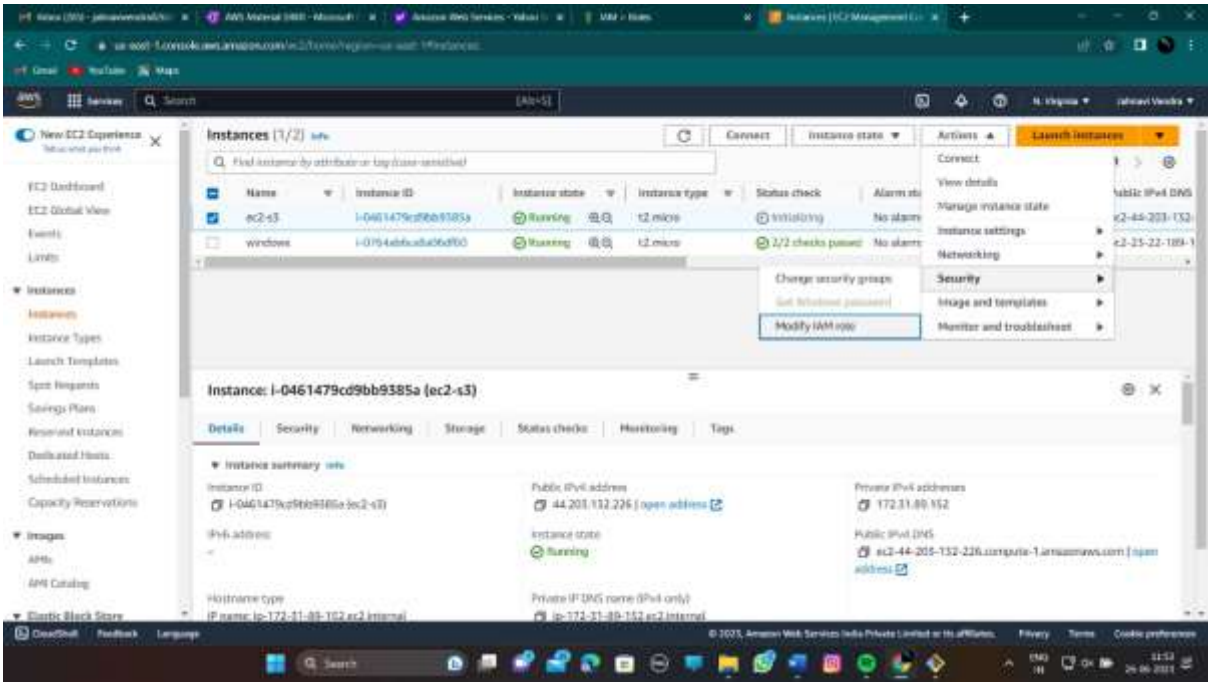
- In the permission policies select AmazonS3FullAccess.



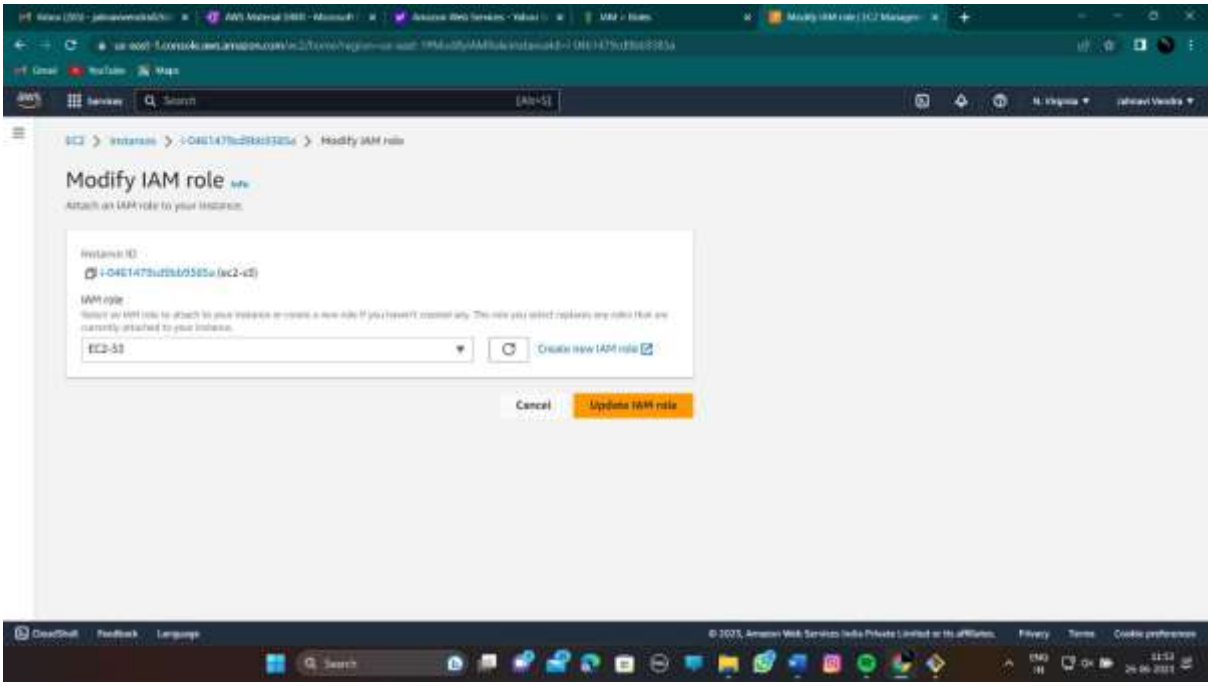
- Here we are given the name as EC2-S3.



- To assign it, simply select the instance and go to actions and select security then you can see Modify IAM role

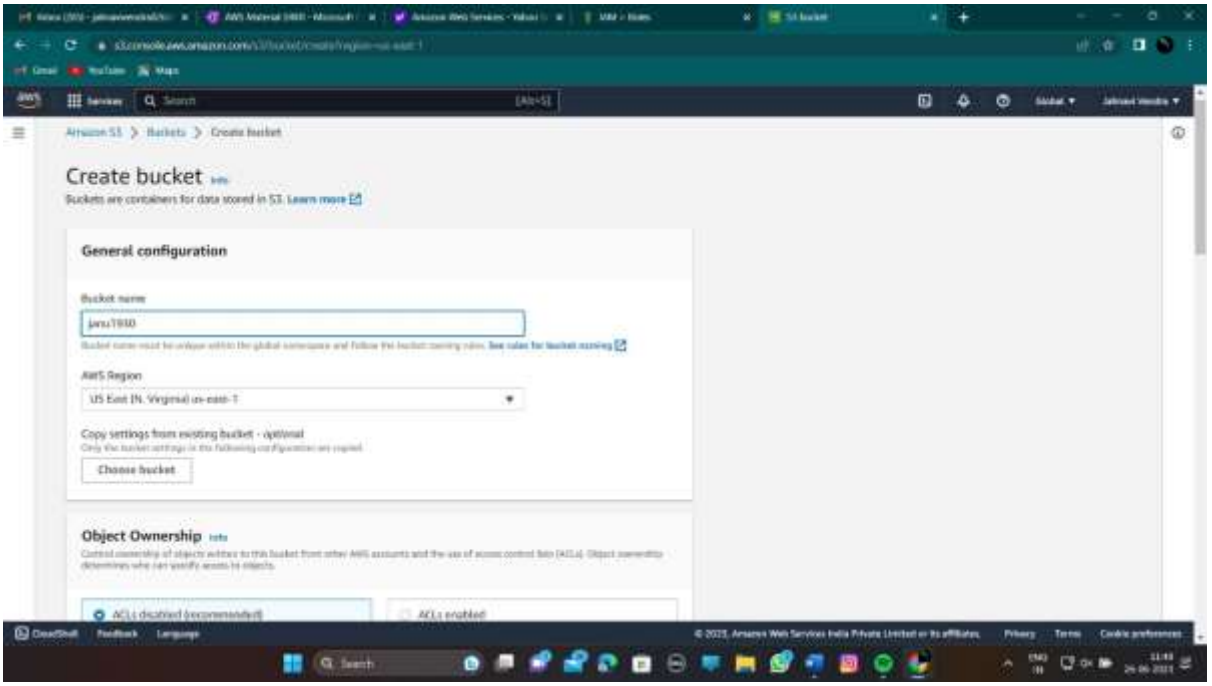


- Select the IAM role which we previously created.

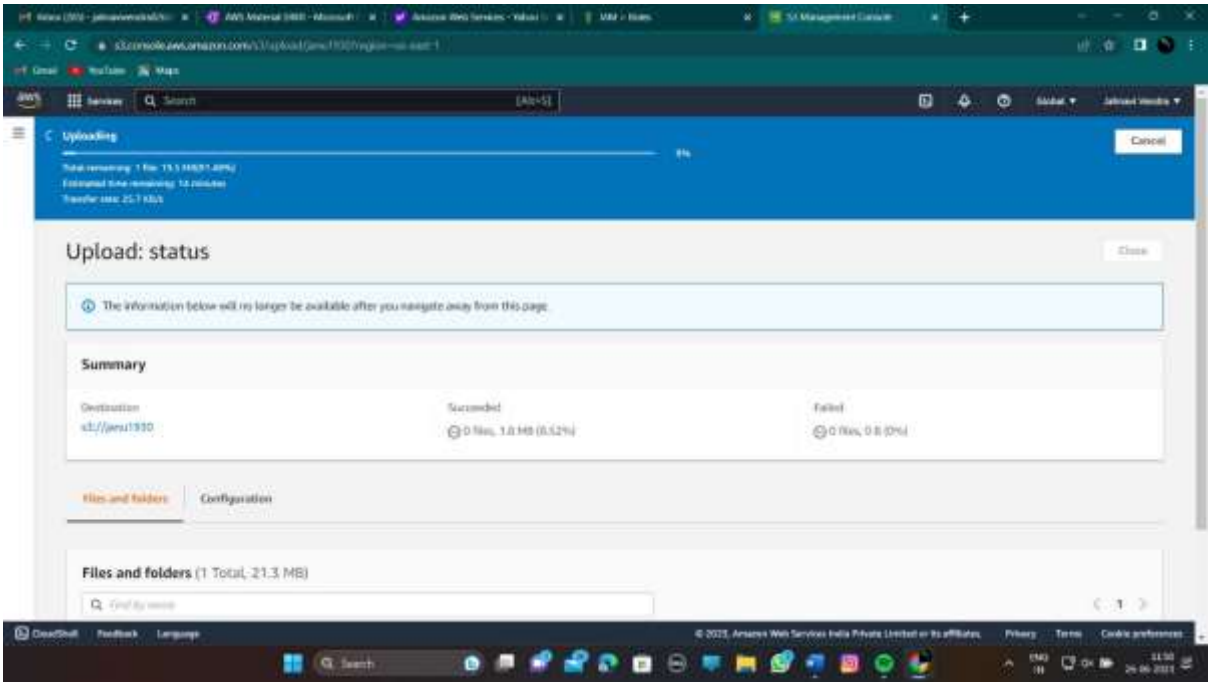


3. **Create an S3 bucket in the console and upload an object.**

- Here we are given the bucket name as follows.

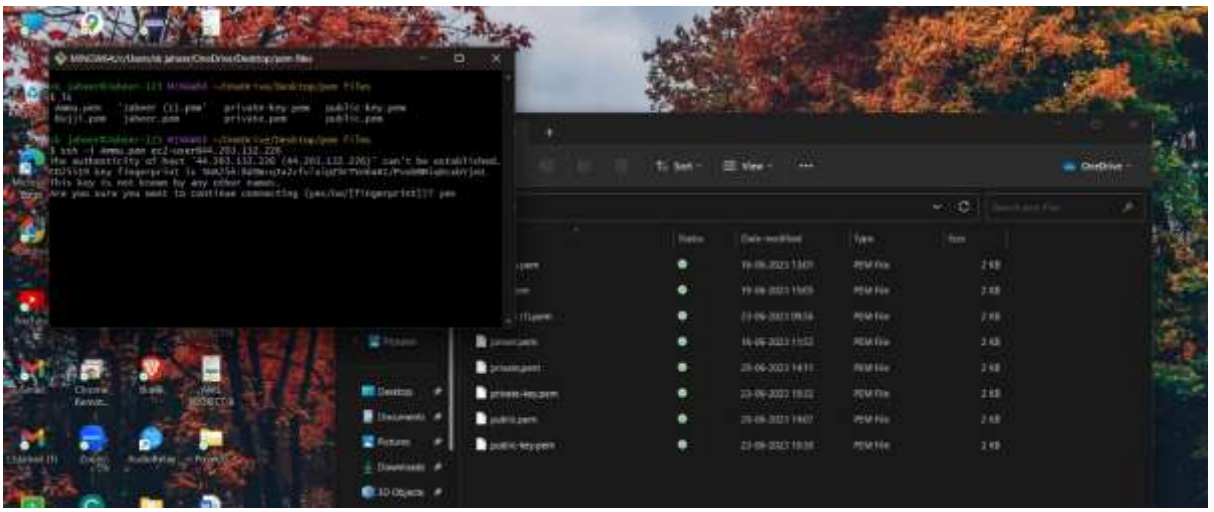


- Now we are uploading an object into the bucket.

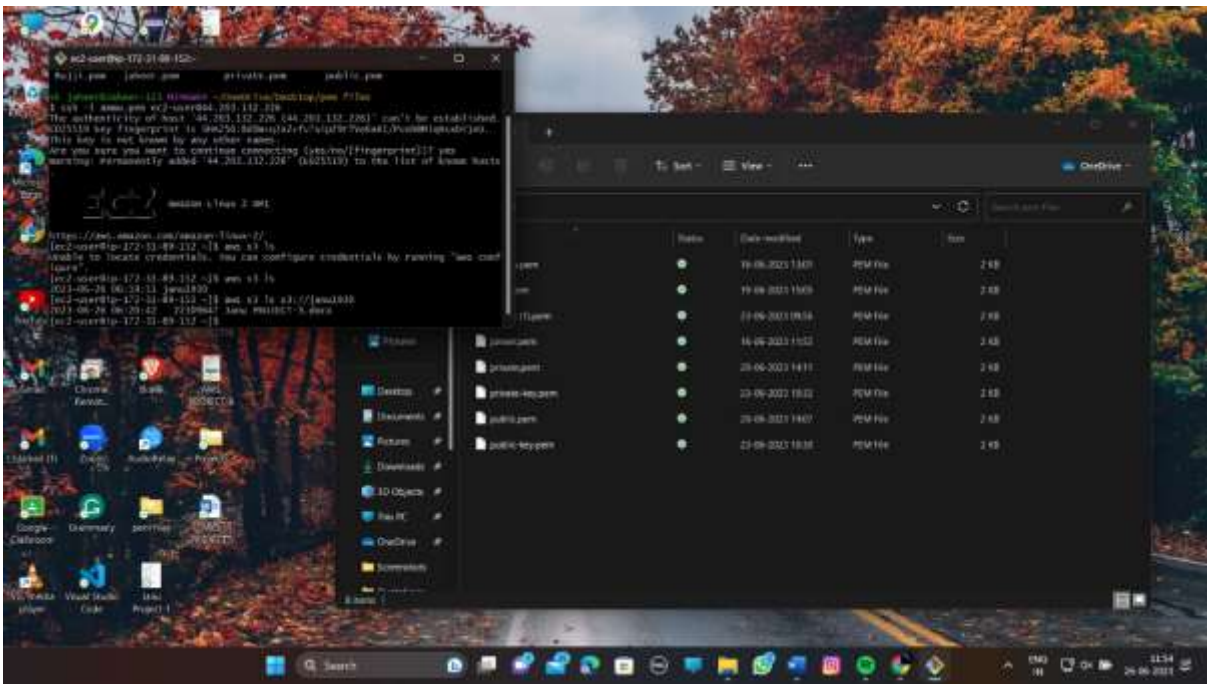


4. Connect to the EC2 instance and run the following commands.

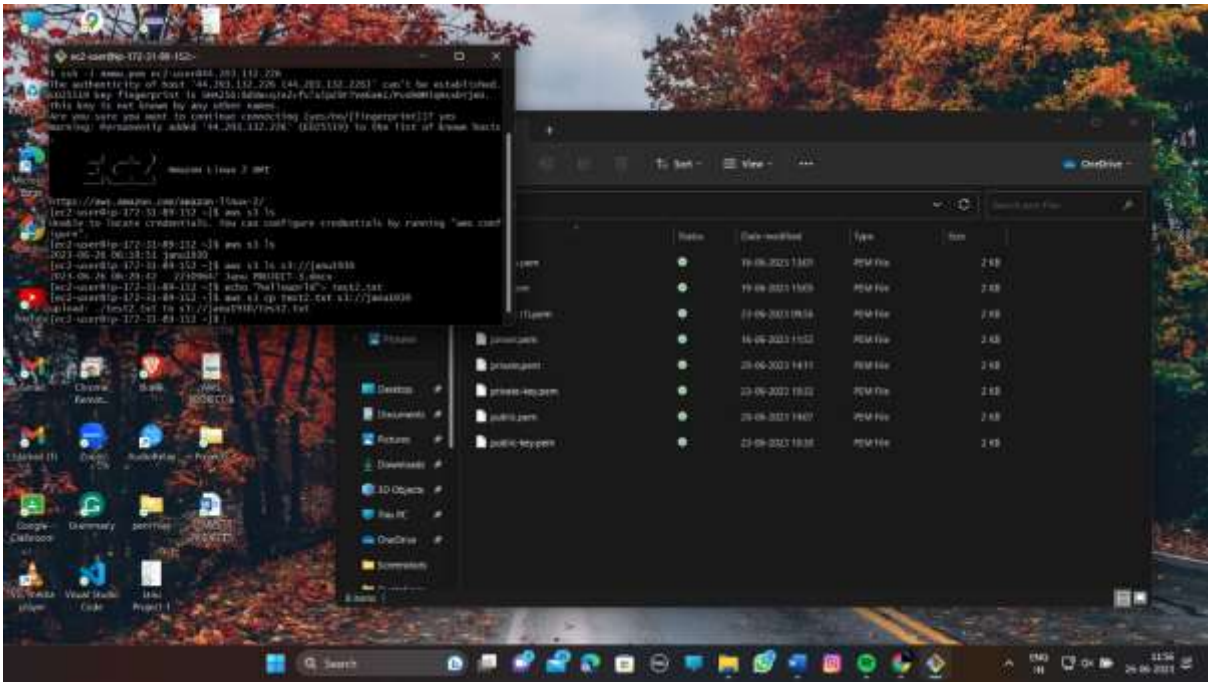
- To establish an SSH connection to the EC2 instance using Git Bash and the .pem file, follow these steps:
- Download Git Bash from any web browser and install it on your computer.
- Once installed, open Git Bash.
- In Git Bash, navigate to the folder where your .pem file is stored. You can use the **cd** command to change directories.
- Change the permissions of the .pem file to ensure it has the correct access rights. Use the **`chmod`** command to modify the permissions.
- Connect to your instance with the public IP of the instance and by using the following commands.
- chmod 400 [PEM file name]
- ssh -i [your.pem] ec2-user@[PUBLIC IP]



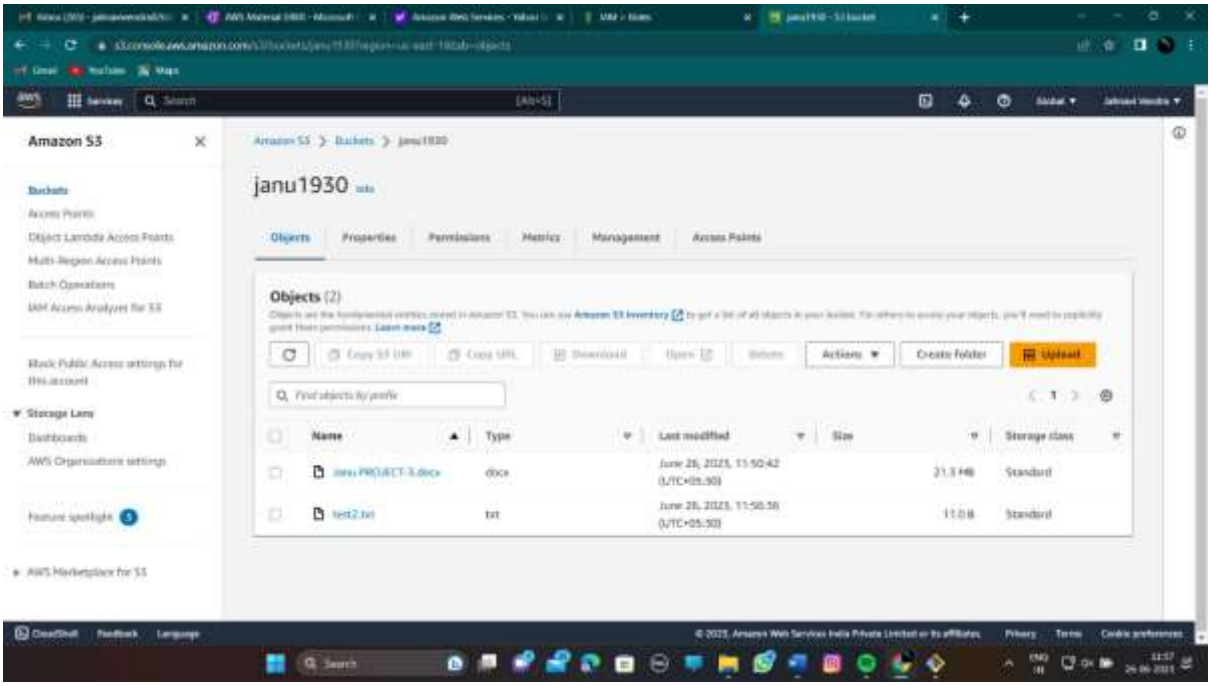
- aws s3 ls --> To display the buckets in S3
- aws s3 ls s3://bucket1 --> To display the contents in the bucket



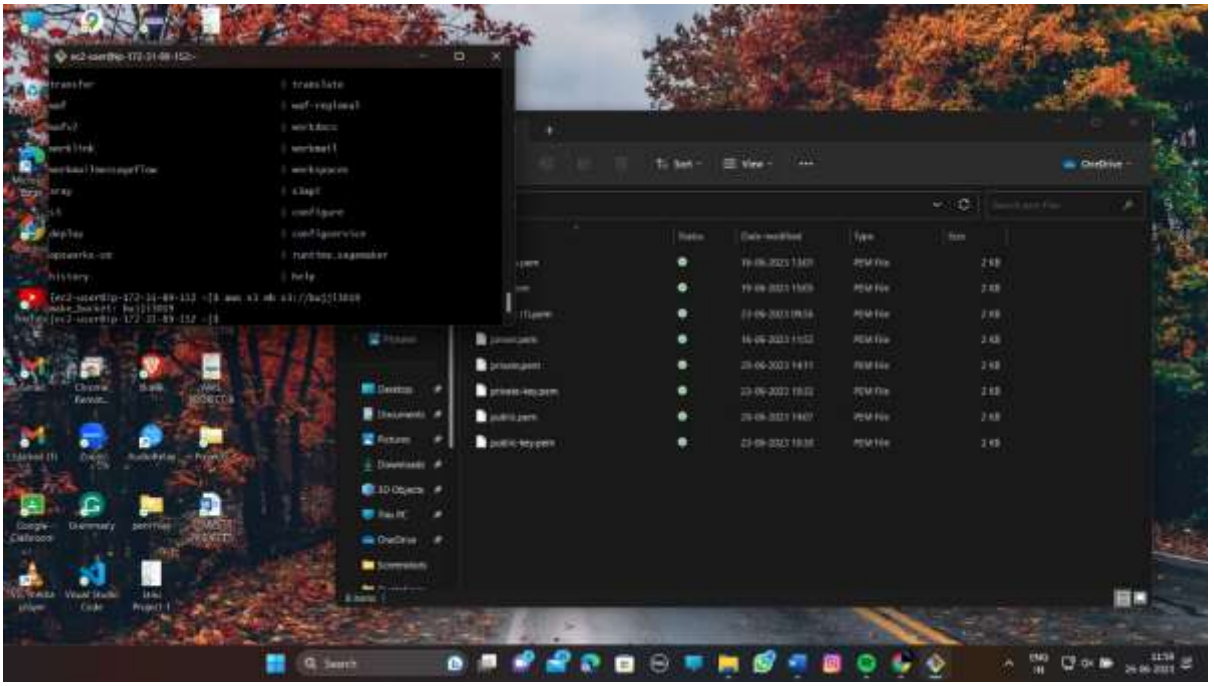
- echo "Hello World" > file1.txt --> To create a text file
- aws s3 cp file1.txt s3://bucket1 --> To copy the text file to S3 bucket



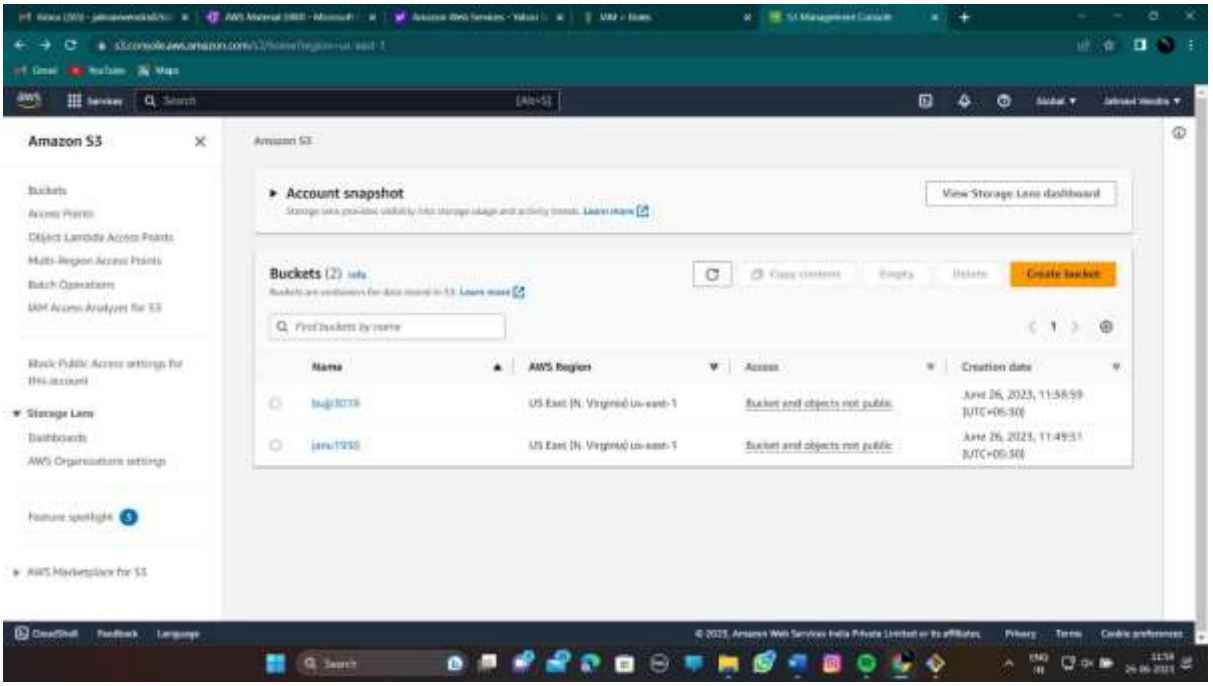
- You can also check in the S3 console.



- aws s3 mb s3://bucket2 --> To create a bucket

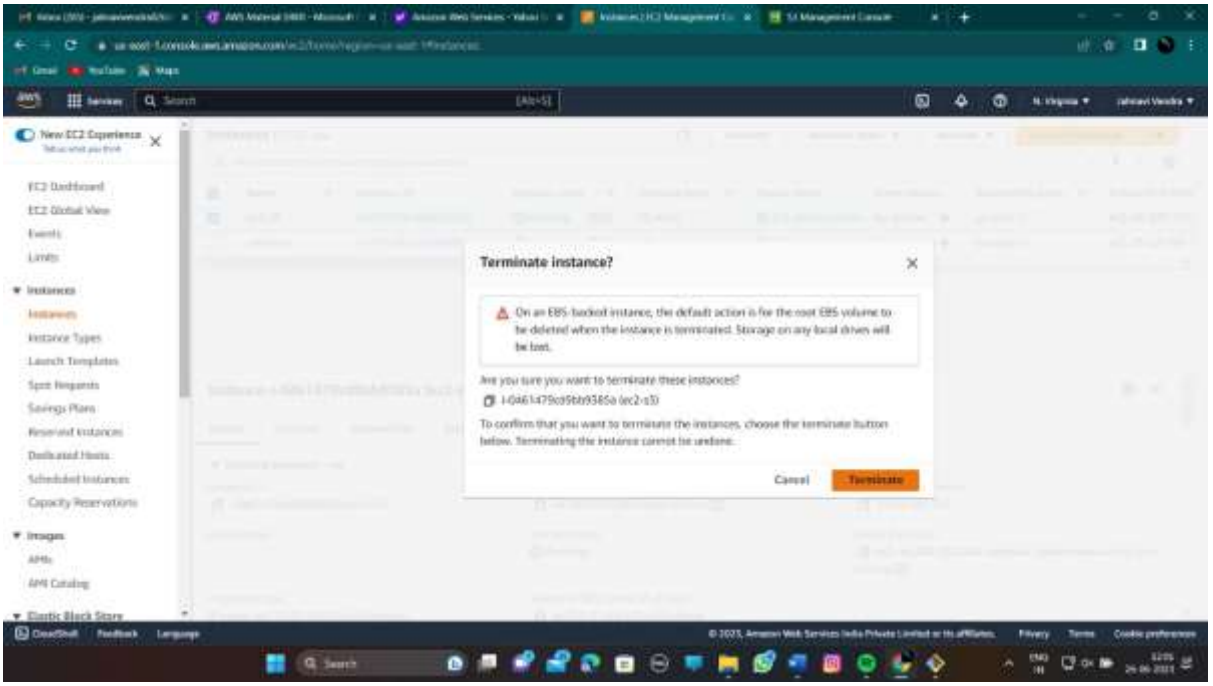


- You can also check in the S3 console.



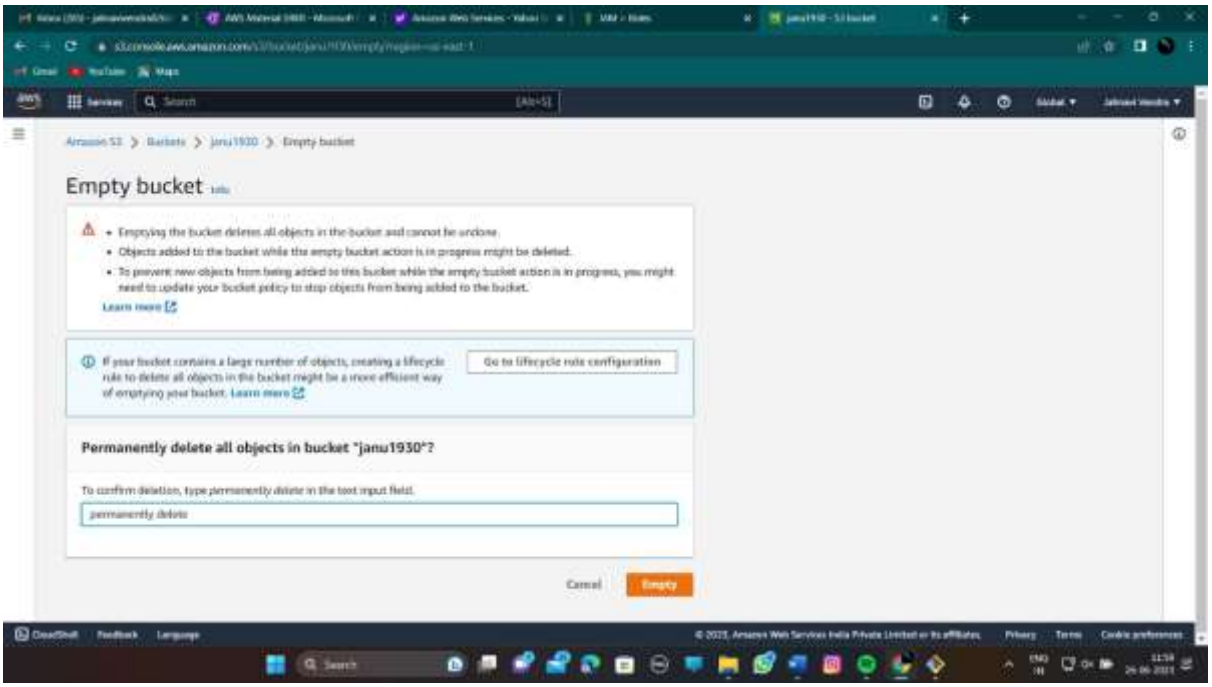
Clean Up :

- Select the checkbox next to the instance name to enable the "Instance state" dropdown menu.
- Click on the "Instance state" dropdown menu and select "Terminate" from the options.
- A confirmation dialog box will appear, displaying information about the termination process and the consequences of terminating the instance.
- Review the information in the confirmation dialog box to ensure you are terminating the correct instance.
- If you are certain you want to proceed with the termination, click on the "Yes, Terminate" button.
- The EC2 instance will enter the termination process. The instance will be shut down, and any associated resources, such as storage volumes, will be deleted. This process may take a few moments.



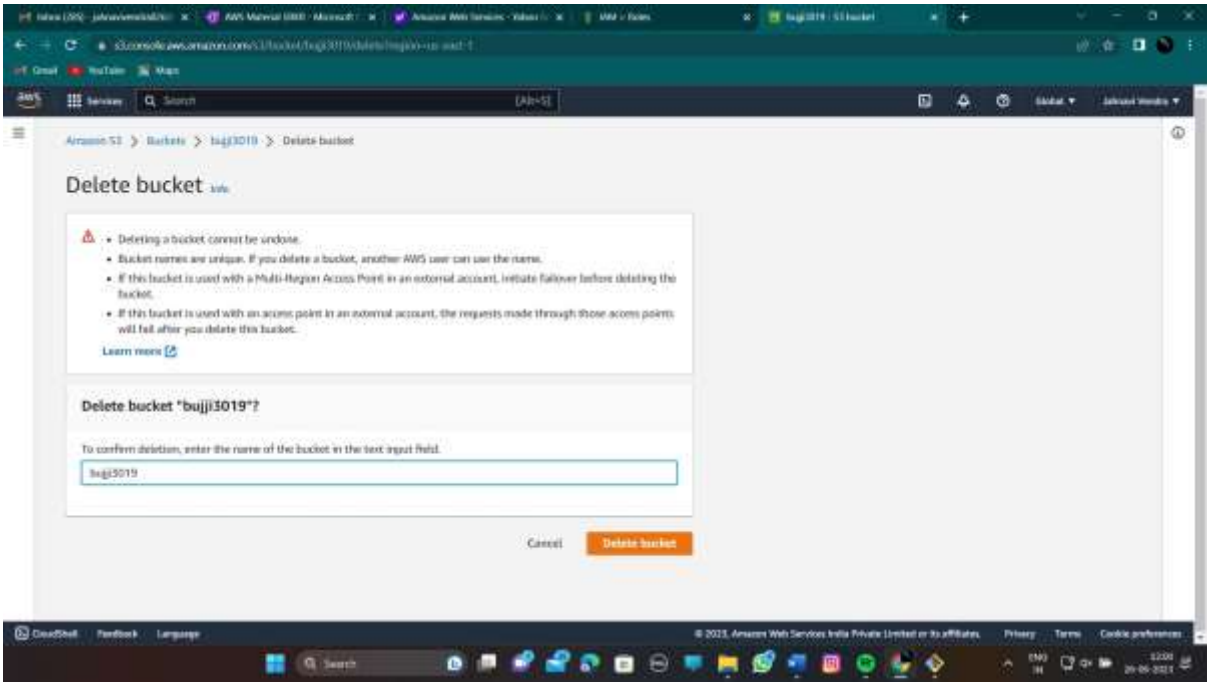
To delete an S3 bucket, you need to empty it first. Follow these steps to empty an S3 bucket before deleting it:

- Go to the Amazon S3 console by signing in to the AWS Management Console and selecting S3 from the services.
- In the S3 console, locate the bucket you want to empty from the list of buckets.
- Click on the name of the bucket to access its contents.
- Select all the objects within the bucket that you want to delete. You can either select individual objects or choose "Select all" to select all objects in the bucket.
- Once the objects are selected, click on the "Actions" dropdown menu and choose "Delete" to remove the selected objects.
- A confirmation dialog box will appear, displaying the number of objects selected for deletion.
- Review the information in the confirmation dialog box to ensure you are deleting the correct objects.



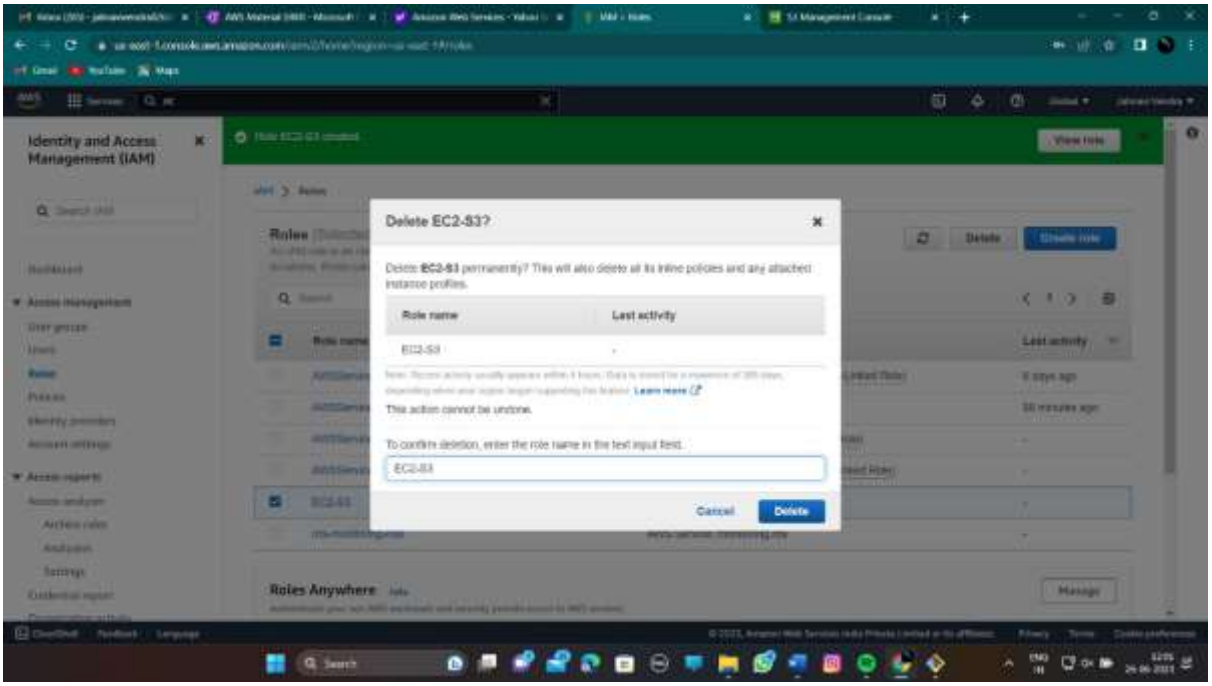
To delete an S3 bucket, follow these steps:

- Go to the Amazon S3 console by signing in to the AWS Management Console and selecting S3 from the services.
- In the S3 console, locate the bucket you want to delete from the list of buckets.
- Select the checkbox next to the bucket name to enable the "Delete" button.
- Click on the "Delete" button at the top of the S3 console.
- A confirmation dialog box will appear, displaying the bucket name and a warning about the irreversible deletion of objects and bucket.
- Review the information in the confirmation dialog box to ensure you are deleting the correct bucket.
- If you are certain you want to proceed with the deletion, type the name of the bucket in the text box provided to confirm.
- Click on the "Delete" button to delete the bucket.



To delete an IAM Role, follow these steps:

- Go to the IAM (Identity and Access Management) console by signing in to the AWS Management Console and selecting IAM from the services.
- In the IAM console, click on "Roles" in the left sidebar.
- Locate the IAM role you want to delete from the list of roles.
- Select the checkbox next to the role name to enable the "Delete role" button.
- Click on the "Delete role" button above the list of roles.
- Click on the "Delete" button to delete the role.



Conclusion:

Performing operations on S3 buckets within an EC2 instance by means of an IAM Role provides secure and efficient access management without the need for explicit credentials within the instance