



BLACKBUCKS INTERNSHIP REPORT

ARCHITECT OF DATA FLOW FROM WEB SERVER TO DATA SERVER

SUBMITTED BY

N PRASANTH KUMAR (21B91A05K7)

K V L SAI KRISHNA(21B91A05F7)

K P C SEKKHAR (21B91A05E5)

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:

- N Prasanth Kumar (21B91A05K7)
- KVL Sai Krishna (21B91A05F7)
- K Poorna Chandra Sekhar(21B91A05E5)

Title:

Architect of dataflow from web server to data server

Abstract:

The architecture describes a data flow that uses AWS services to move data from an EC2 instance to an S3 bucket, then to an RDS database, and then to a read replica of that database. The data can then be accessed from another EC2 instance.

The data flow is designed to be scalable, secure, and flexible. It can be used to process a variety of data types, and it can be scaled to handle large volumes of data. The data is stored in S3 and RDS, which are both secure services. The data can be accessed from multiple EC2 instances, which allows for flexibility in how the data is used.

Table of Contents

1. Introduction to Amazon web services (AWS)	4-5
2. Why AWS	5-8
3. AWS global Infrastructure	8-11
4. List of top AWS services	11-21
5. Implementation of the Architecture	22
5.1. AWS services used	22
5.2. Rough Architecture	22
5.3. Final Architecture	23
6. Implementation of the project	24
6.1. Service 1: VPC	24-30
6.2. Service 2: EC2	30-32
6.3. Service 3: S3	32-34
6.4. Service 4: IAM	35-38
6.5. Service 5: RDS	39-42
6.6. Service 5.1: Read Replica	43-45
6.7. Service 2.1: EC2 (Singapore)	46-47
6.7. Conclusion	52

Introduction To Amazon Web Services (AWS):

- **Amazon Web Services, Inc. (AWS)** is a subsidiary of Amazon that provides on-demand 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-you-go" 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

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

unpredictable or very high loads. Due to this reason, organizations enjoy the benefits of reduced cost and increased user satisfaction.

4) Security

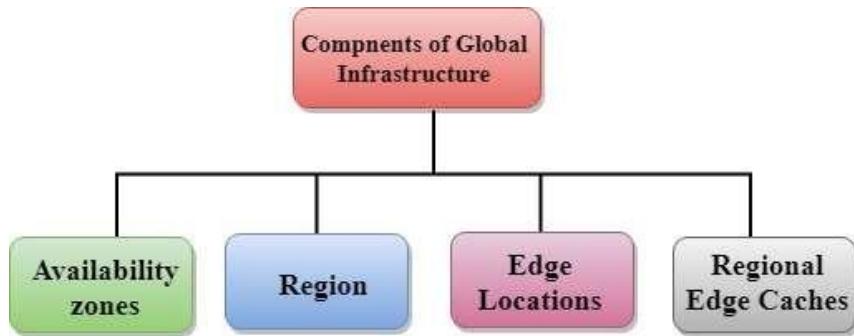
- AWS provides end-to-end security and privacy to customers.
- AWS has a virtual infrastructure that offers optimum availability while managing full privacy and isolation of their operations.
- Customers can expect high-level physical security because of Amazon's several years of experience in designing, developing, and maintaining large-scale IT operation centers.
- AWS ensures the three aspects of security, i.e., Confidentiality, integrity, and availability of users.

AWS Global Infrastructure

- 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.

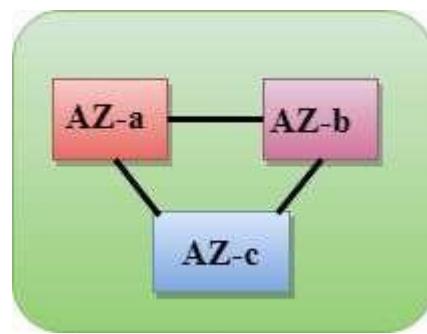
High availability: Distributing resources across AZs allows you to achieve high availability for your applications. Services like load balancers can be configured to route traffic across multiple AZs, automatically diverting traffic to healthy instances if one AZ becomes unavailable.

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, cost-effective 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 on-premise 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 auto-scaling 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 in-memory 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.



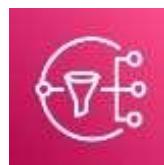
14. Amazon Sagemaker

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 high-performance workloads such as SAP, Oracle, and Microsoft products. And it provides better

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 pre-defined 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

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 fulfill compliance and regulatory requirements.

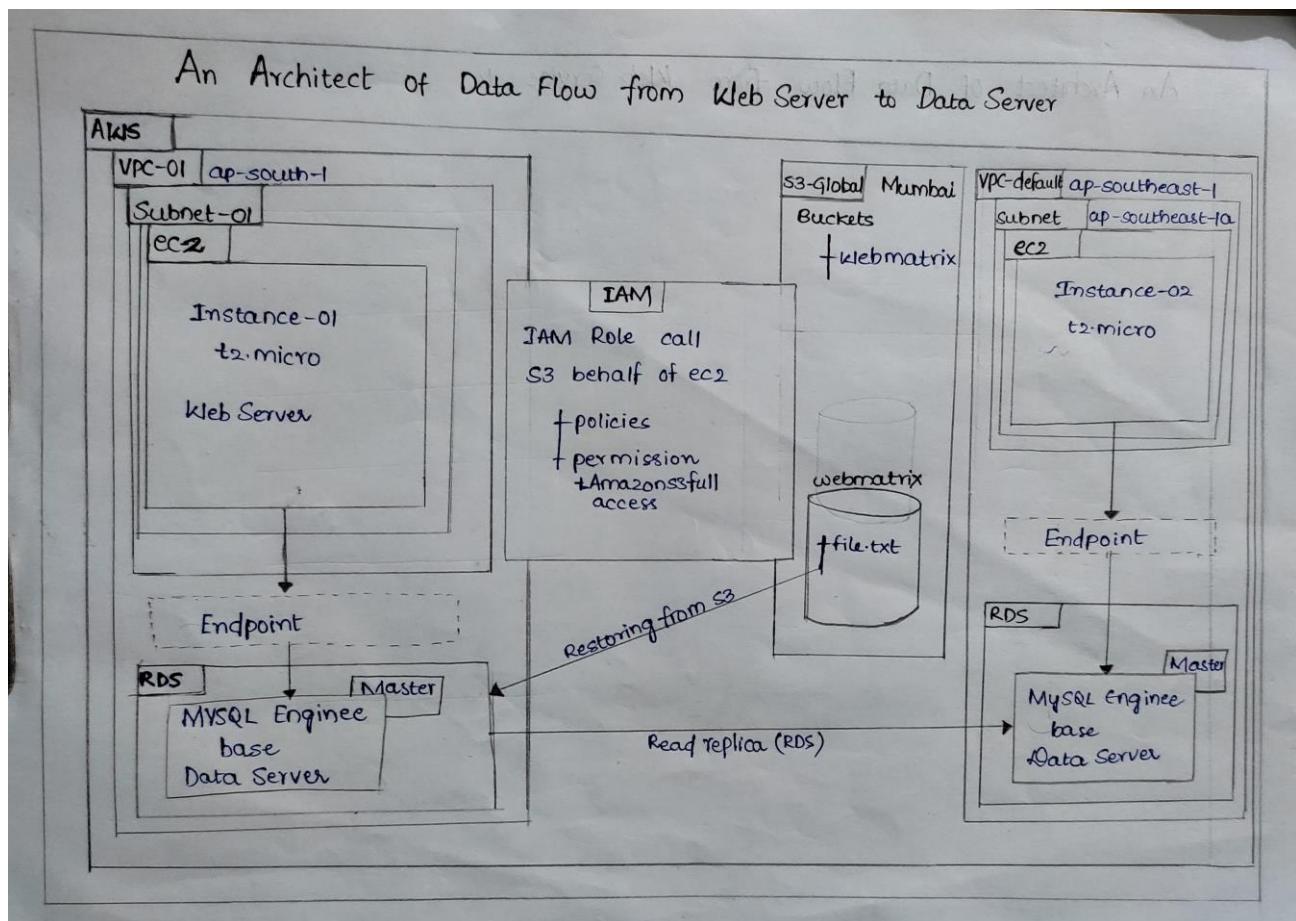


5. IMPLEMENTATION OF ARCHITECTURE

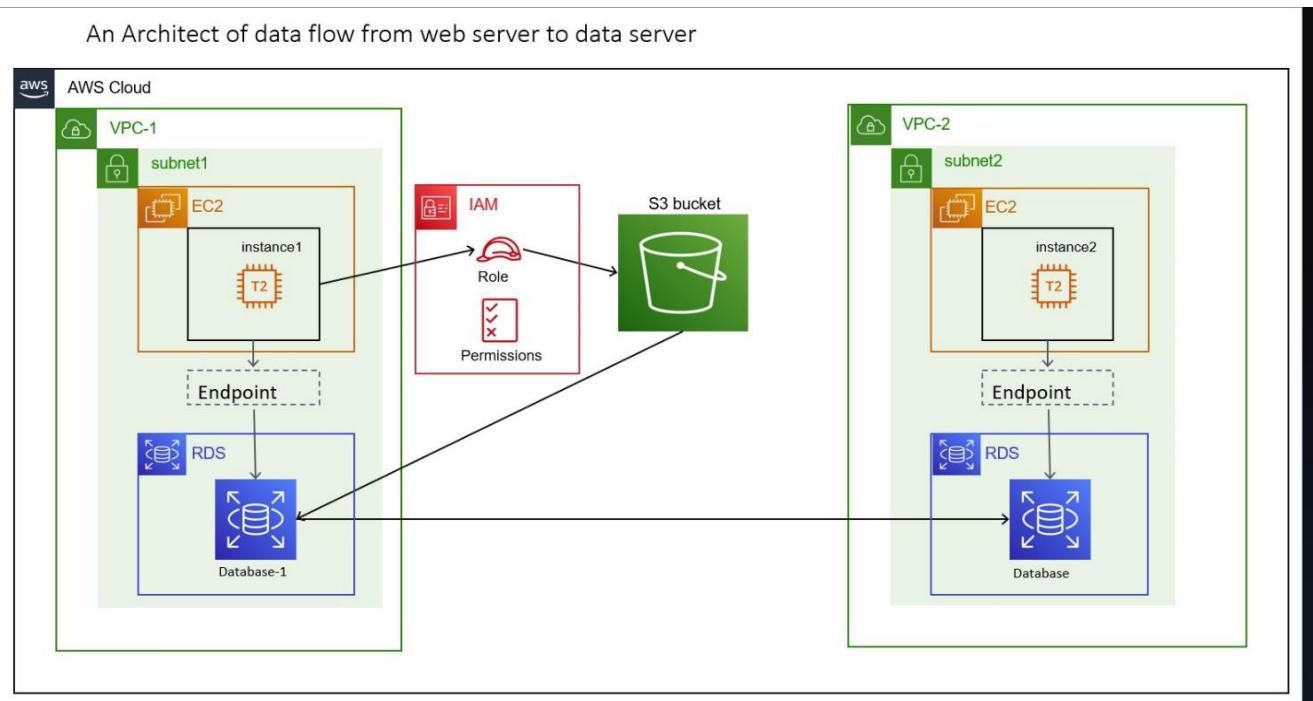
Services used:

- EC2 (Elastic Compute Cloud)
- VPC (Virtual Private Cloud)
- S3(Simple Storage Service)
- RDS(Relational Database Service)
- IAM(Identity And Access Management)
- Read Replica

Rough architecture:



Final architecture:



IMPLEMENTATION

Service 1: VPC

Steps to perform:

- Go to the AWS Management Console and sign in to your account.
- In the AWS Management Console, click the VPC service.
- In the VPC dashboard, click the Create VPC button.
- In the Name field, enter vpc-1.
- In the IPv4 CIDR block field, enter 10.0.0.0/24.

A screenshot of the AWS VPC Create VPC Info page. The top navigation bar shows 'Services' and 'Search'. Below it, 'VPC' is selected in the breadcrumb trail. The main form has a title 'Create VPC Info'. It contains sections for 'VPC settings', 'Resources to create' (radio buttons for 'VPC only' and 'VPC and more' with 'VPC only' selected), 'Name tag - optional' (text input 'vpc-01'), 'IPv4 CIDR block' (radio buttons for 'IPv4 CIDR manual input' and 'IPAM-allocated IPv4 CIDR block' with 'IPv4 CIDR manual input' selected), and 'IPv4 CIDR' (text input '10.0.0.0/24'). A sidebar on the right shows 'Your VPCs'.

- Click the Create button

A screenshot of the AWS VPC Create VPC page after clicking 'Create'. The top navigation bar shows 'Services' and 'Search'. Below it, 'VPC' is selected in the breadcrumb trail. The main form has sections for 'IPv6 CIDR block' (radio buttons for 'No IPv6 CIDR block', 'IPAM-allocated IPv6 CIDR block', 'Amazon-provided IPv6 CIDR block', and 'IPv6 CIDR owned by me' with 'No IPv6 CIDR block' selected), 'Tenancy' (dropdown 'Default'), 'Tags' (table with one row 'Name: vpc-01'), and 'Key' (text input 'Name') and 'Value - optional' (text input 'vpc-01'). At the bottom are 'Cancel' and 'Create VPC' buttons, with 'Create VPC' highlighted.

- Once the VPC has been created, you can verify that it was created successfully by checking the VPCs page in the AWS Management Console.
- The VPC should be listed with the name `vpc-1` and the IPv4 CIDR block `10.0.0.0/24`.

The screenshot shows the AWS Management Console VPC dashboard. At the top, there's a navigation bar with the AWS logo, services like S3, EC2, Billing, VPC, IAM, and RDS, and a search bar. Below the navigation bar, the main title is "Your VPCs (1) Info". A table lists one VPC entry:

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
vpc-01	vpc-095db84d33c8b4249	Available	10.0.0.0/24	-

On the left side, there's a sidebar titled "Virtual private cloud" with a "Your VPCs" section containing links for Subnets, Route tables, Internet gateways, Egress-only internet gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, and NAT gateways. At the bottom of the page, there are CloudShell, Feedback, Language, and cookie preferences links.

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

The screenshot shows the AWS Management Console Route tables page. At the top, there's a navigation bar with the AWS logo, services like S3, EC2, Billing, VPC, IAM, and RDS, and a search bar. Below the navigation bar, the main title is "Route tables (1/2) Info". A table lists two route tables:

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
-	rtb-0a25c82b261608adc	-	-	Yes	vpc-095db84d33c8b4249
<input checked="" type="checkbox"/> rt1-vpc1	rtb-05f56fffa481ec6eb	-	-	Yes	vpc-095db84d33c8b4249

Below the table, there's a detailed view for the selected route table "rt1-vpc1". It shows the ID "rtb-05f56fffa481ec6eb / rt1-vpc1" and tabs for Details, Routes, Subnet associations, Edge associations, Route propagation, and Tags. A message says "You can now check network connectivity with Reachability Analyzer" with a "Run Reachability Analyzer" button. At the bottom, there are CloudShell, Feedback, Language, and cookie preferences links.

- In the VPC dashboard, click the Subnets tab.
- Click the Create subnet button.

The screenshot shows the 'Create subnet' page in the AWS VPC console. In the 'VPC' section, the 'VPC ID' dropdown is set to 'vpc-095db84d33c8b4249 (vpc-01)'. Under 'Associated VPC CIDRs', the IPv4 CIDR is listed as '10.0.0.0/24'.

- In the Name field, enter subnet1.
- In the Availability Zone drop-down list, select ap-south-1a.
- In the IPv4 CIDR block field, enter 10.0.0.0/25.

The screenshot shows the 'Subnet 1 of 1' configuration page. The 'Subnet name' is set to 'subnet-1'. The 'Availability Zone' is set to 'Asia Pacific (Mumbai) / ap-south-1a'. The 'Use' dropdown shows '10.0.0.0/25' and the input field also contains '10.0.0.0/25'. A tag 'Name' with value 'subnet-1' is added under 'Tags - optional'.

- Click the Create button.
- also create a subnet with the name subnet2, the availability zone ap-south-1b, and the CIDR block 10.0.0.128/25.

The screenshot shows the AWS Management Console with the VPC service selected. A modal window titled "Subnet 2 of 2" is open for creating a new subnet. The "Subnet name" field contains "subnet-2". The "Availability Zone" dropdown is set to "Asia Pacific (Mumbai) / ap-south-1b" and the "Use" dropdown is set to "10.0.0.128/25". A tag named "Name" with value "subnet-2" is added. The "IPv4 CIDR" field is empty. The "Actions" dropdown menu is visible at the top right of the modal.

- Once the subnets have been created, you can verify that they were created successfully by checking the Subnets page in the AWS Management Console.
- The subnets should be listed with the names subnet1 and subnet2, the availability zones ap-south-1a and ap-south-1b, and the CIDR blocks 10.0.0.0/25 and 10.0.0.128/25, respectively.

The screenshot shows the AWS Management Console with the VPC service selected. A success message at the top states "You have successfully created 2 subnets: subnet-018fd94aa2ac9cb78, subnet-0cff2446763b33843". Below it, a table lists five subnets:

Name	Subnet ID	State	VPC	IPv4 CIDR
-	subnet-07424e93ab5df09d5	Available	vpc-0b1ebd6052cb5f516	172.31.0.0/2
-	subnet-0398bb8c1d08dd075	Available	vpc-0b1ebd6052cb5f516	172.31.32.0/
-	subnet-07e063de42af5b094	Available	vpc-0b1ebd6052cb5f516	172.31.16.0/
subnet-2	subnet-0cff2446763b33843	Available	vpc-095db84d33c8b4249 vpc-...	10.0.0.128/2
subnet-1	subnet-018fd94aa2ac9cb78	Available	vpc-095db84d33c8b4249 vpc-...	10.0.0.0/25

- Select your VPC: Choose the VPC "VPC-1" that you created earlier.
- Go to route tables and edit the subnet associations and select subnet1 and subnet2 and click on save associations.

- Create an internet gateway with the name igw-01.

Create internet gateway [Info](#)

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.

Tags - optional
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="igw-01"/> Remove

[Add new tag](#)

[CloudShell](#) [Feedback](#) [Language](#) © 2023, Amazon Web Services India Private Limited or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

- Attach custom IGW to custom VPC.

The following internet gateway was created: igw-0693b61837e360566 - igw-01. You can now attach to a VPC to enable the VPC to communicate with the internet. [Attach to a VPC](#)

VPC dashboard [X](#) [Services](#) [Search](#) [Alt+S] Mumbai Prasanth Kumar Nagulapalli

EC2 Global View [New](#)

Filter by VPC: [Select a VPC](#)

Virtual private cloud

Your VPCs [New](#)

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

igw-0693b61837e360566 / igw-01

[Actions](#)

Details [Info](#)

Internet gateway ID igw-0693b61837e360566	State Detached	VPC ID -	Owner 371206070807
--	-----------------------------------	-------------	---------------------------------------

Tags [Manage tags](#)

Key	Value
Name	igw-01

[CloudShell](#) [Feedback](#) [Language](#) © 2023, Amazon Web Services India Private Limited or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

The screenshot shows the 'Attach to VPC' dialog box for an Internet Gateway (igw-0693b61837e360566). It displays a list of available VPCs, with 'vpc-02652007df96b1b23 - vpc-01' selected. A large orange 'Attach internet gateway' button is at the bottom right.

- Internet Gate Way is successfully attached to VPC.

The screenshot shows the 'Internet gateways (2)' list. It displays two entries: 'igw-01' and another entry with a placeholder name. Both are attached to the VPC 'vpc-02652007df96b1b23 | vpc-01'. An orange 'Create internet gateway' button is visible at the top right.

- Now go to route tables, select rt1-vpc1, click on edit routes, go to add routes, and add 0.0.0.0/0 at destination and select our internet gateway in target and save it.

The screenshot shows the 'Edit routes' dialog box for a specific route table. It lists two routes: one to 'local' and another to 'igw-0693b61837e360566'. A large orange 'Save changes' button is at the bottom right.

Service 2: EC2

Steps to perform:

- In the AWS Management Console, click the EC2 service.
- Name your instance as instance-01,

The screenshot shows the 'Launch an instance' wizard in the AWS Management Console. The top navigation bar includes the AWS logo, Services, Search, and Mumbai region. The main section is titled 'Launch an instance' with a sub-section 'Name and tags'. The 'Name' field contains 'instance-01'. To the right, a 'Summary' panel shows the configuration: 1 instance, Amazon Linux 2 Kernel 5.10 AMI, t2.micro instance type, New security group, and 1 volume(s) - 8 GiB. A large orange 'Launch instance' button is prominent at the bottom right of the summary panel.

- Select “amazon linux 2 ami (hvm) - kernel 5.10 ssd volume type”.
- Instance type “t2. micro”.
- Select your existing key pair.

The screenshot shows the 'Instance type' configuration step in the 'Launch an instance' wizard. The 't2.micro' instance type is selected, showing details like 1 vCPU, 1 GiB Memory, and Current generation: true. The 'Key pair (login)' section shows 'SSAI' selected. The 'Network settings' section is partially visible. The right side of the screen displays the same 'Summary' panel as the previous screenshot, showing 1 instance, Amazon Linux 2 Kernel 5.10 AMI, t2.micro instance type, New security group, and 1 volume(s) - 8 GiB. The 'Launch instance' button is again highlighted.

- Select your custom VPC, public subnet and enable the auto-assign public IP.
- In the security group section, select availability zone as south-1a.

Network settings

VPC - required info
vpc-095db84d33cb4249 (vpc-01)
10.0.0.0/24

Subnet info
subnet-018fd94aa2ac9cb78
VPC: vpc-095db84d33cb4249 Owner: 151754574085 Availability Zone: ap-south-1a IP addresses available: 123 CIDR: 10.0.0.0/24

Create new subnet

Auto-assign public IP info
Enable

Firewall (security groups) info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group (radio button selected)

Select existing security group (radio button unselected)

Security group name - required
sai_sg

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 _-:/@#=;&|\$^

Cancel Launch instance Review commands

- create a new security group, add security groups that supports SSH and all the traffic.

Inbound Security Group Rules

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

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 X ::/0 X

Remove

Security group rule 2 (All, All, Multiple sources)

Type info: All traffic, Protocol info: All, Port range info: All

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 X ::/0 X

Remove

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting a more restrictive rule. X

CloudShell Feedback Language

Number of instances Info
1

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel Launch instance Review commands

Add security group rule

Advanced network configuration

Configure storage info

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 X

Add new volume

0 x File systems Edit

Advanced details info

Number of instances Info
1

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel Launch instance Review commands

- Launch your instance.

The screenshot shows the AWS EC2 Instances page. The top navigation bar includes the AWS logo, services like S3, EC2, Billing, VPC, IAM, and RDS, a search bar, and account information for Mumbai and Sai Krishna. On the left, a sidebar menu is open under 'Instances' with options like Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, and Capacity Reservations. The main content area displays a table titled 'Instances (1) Info' with one row for 'instance-01'. The table columns include Name, Instance ID, Instance state, Instance type, Status check, Alarm status, and Availability Zone. The instance 'instance-01' is listed with an Instance ID of i-0737de746e62598ca, an Instance state of Running, an Instance type of t2.micro, a Status check of Initializing, and an Availability Zone of ap-south-1a. Below the table, a modal window titled 'Select an instance' is open, showing the same instance information. The bottom of the screen has standard AWS footer links for CloudShell, Feedback, Language, and cookie preferences.

Service 3:S3

Steps to perform:

- In the AWS Management Console, click the S3 service.
- In the S3 dashboard, click the Create Bucket button.
- In the Bucket Name field, enter Webmatrix.
- In the Region drop-down list, select ap-south-1.

The screenshot shows the 'Create bucket' configuration page in the AWS S3 service. The top navigation bar includes the AWS logo, services like S3, EC2, Billing, VPC, IAM, and RDS, a search bar, and account information for Global and Sai Krishna. The main form is titled 'Create bucket' with a 'General configuration' section. It contains fields for 'Bucket name' (set to 'webmatrix'), 'AWS Region' (set to 'Asia Pacific (Mumbai) ap-south-1'), and a 'Copy settings from existing bucket - optional' section with a 'Choose bucket' button. Below this is an 'Object Ownership' section with a note about controlling object ownership and access control lists (ACLs). It features two radio buttons: 'ACLs disabled (recommended)' and 'ACLs enabled' (which is selected). The bottom of the screen has standard AWS footer links for CloudShell, Feedback, Language, and cookie preferences.

- In the Object Ownership section, select the ACLs enabled.

The screenshot shows the 'Object Ownership' section of the AWS S3 console. It includes two radio button options: 'ACLs disabled (recommended)' and 'ACLs enabled'. A warning message states: 'We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.' Below this, there are sections for 'Object Ownership' and 'Bucket owner preferred' (selected), which notes that new objects are owned by the bucket owner. There is also a note about enforcing ownership via bucket policy.

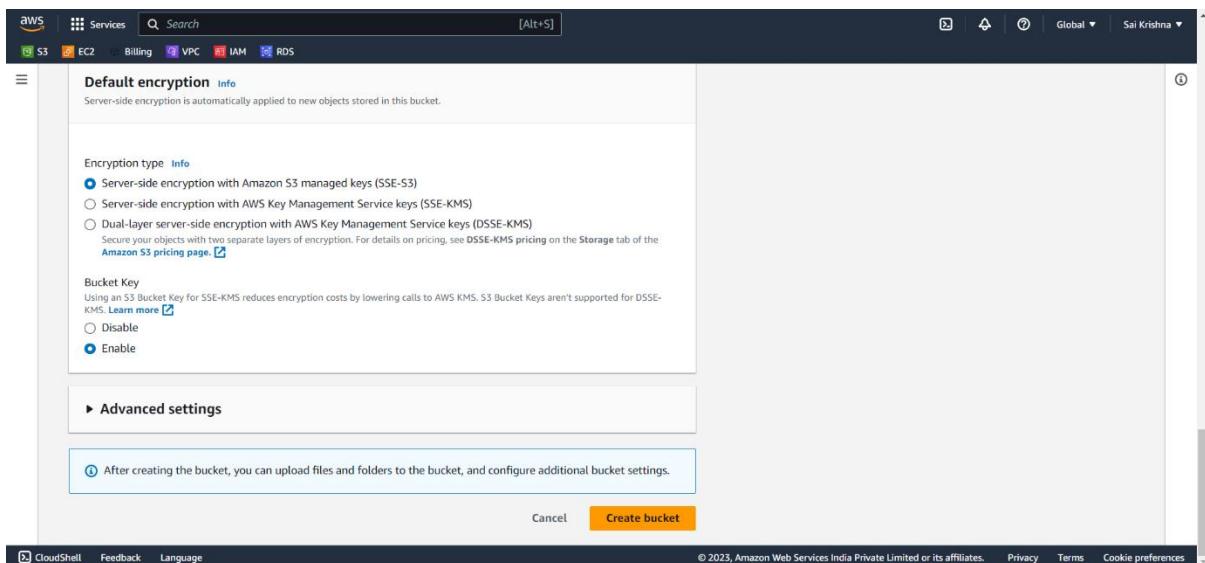
- In the Block Public Access section, uncheck the Block all public access checkbox.

The screenshot shows the 'Block Public Access settings for this bucket' section. It lists four checkboxes under 'Block all public access': 'Block public access to buckets and objects granted through new access control lists (ACLS)', 'Block public access to buckets and objects granted through any access control lists (ACLS)', 'Block public access to buckets and objects granted through new public bucket or access point policies', and 'Block public and cross-account access to buckets and objects through any public bucket or access point policies'. A warning message at the bottom states: 'Turning off block all public access might result in this bucket and the objects within becoming public. AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.'

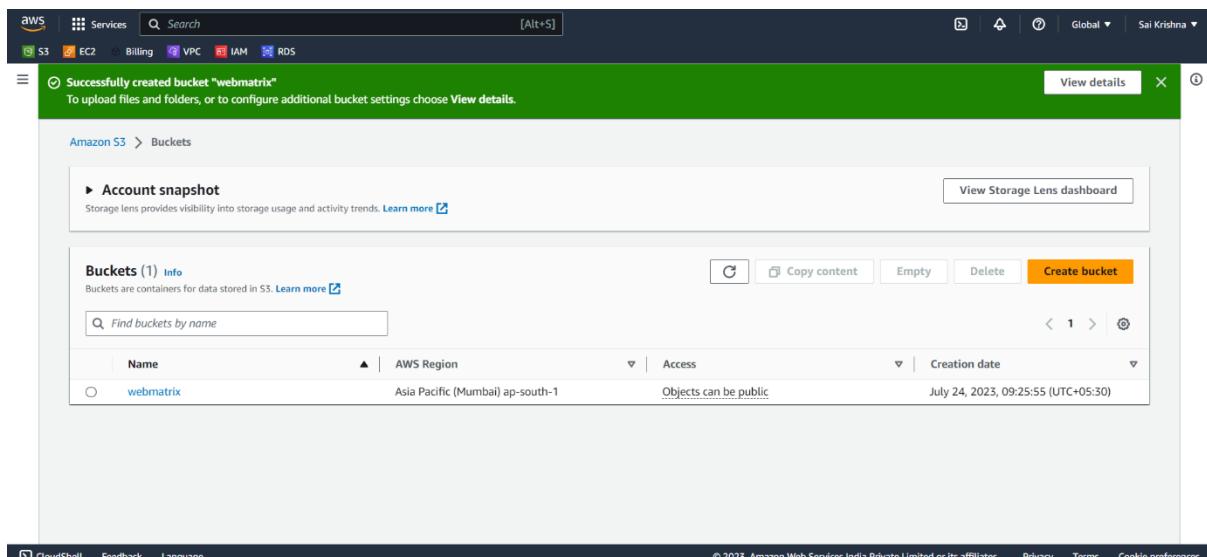
- In the Versioning section, select the Enable option.

The screenshot shows the 'Bucket Versioning' section. It contains a note: 'Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more.' Below this, there is a 'Bucket Versioning' section with a radio button for 'Enable' (selected) and a note: 'Server-side encryption is automatically applied to new objects stored in this bucket.'

- Click the Create button.



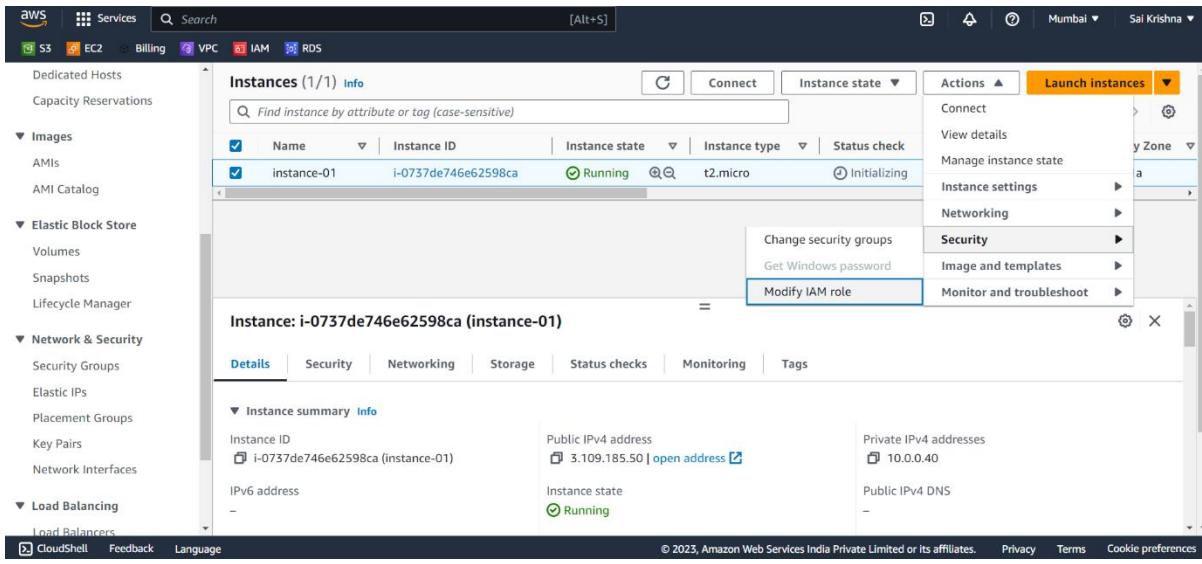
- Once the bucket has been created, you can verify that it was created successfully by checking the Buckets page in the AWS Management Console.
- The bucket should be listed with the name webmatrix, the region ap-south-1.



service 3: IAM

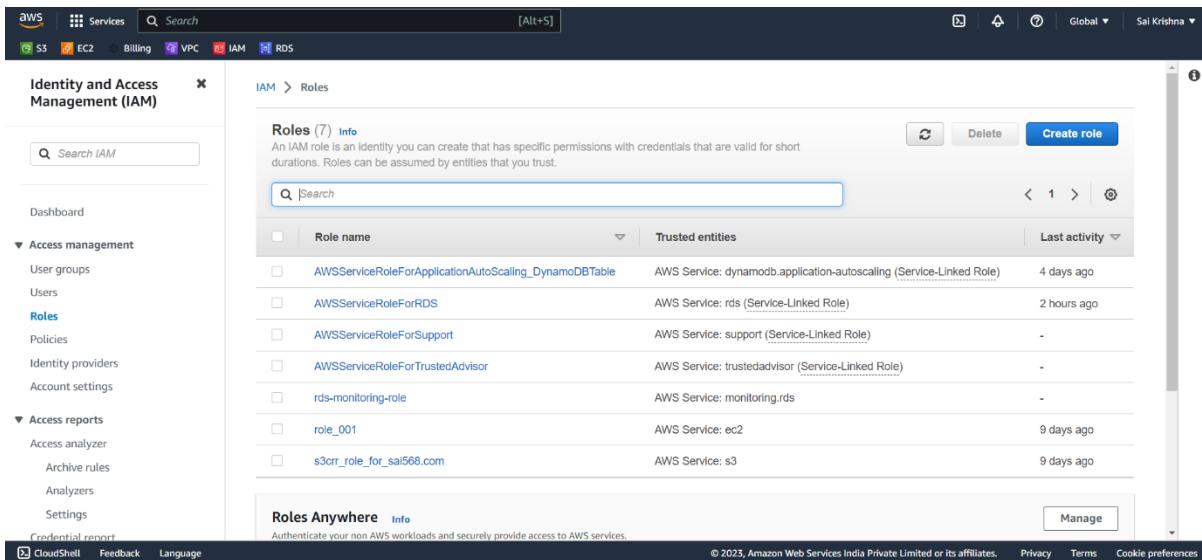
Steps to perform:

- In the AWS Management Console, click the IAM service.



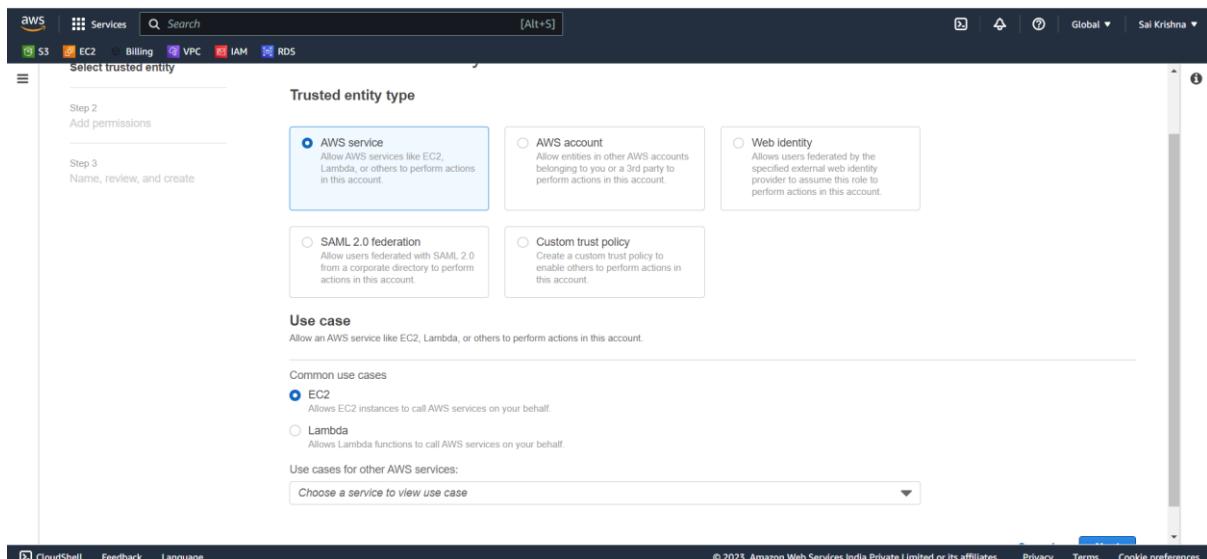
- In the IAM dashboard, click the Roles tab.

- Click the Create role button.

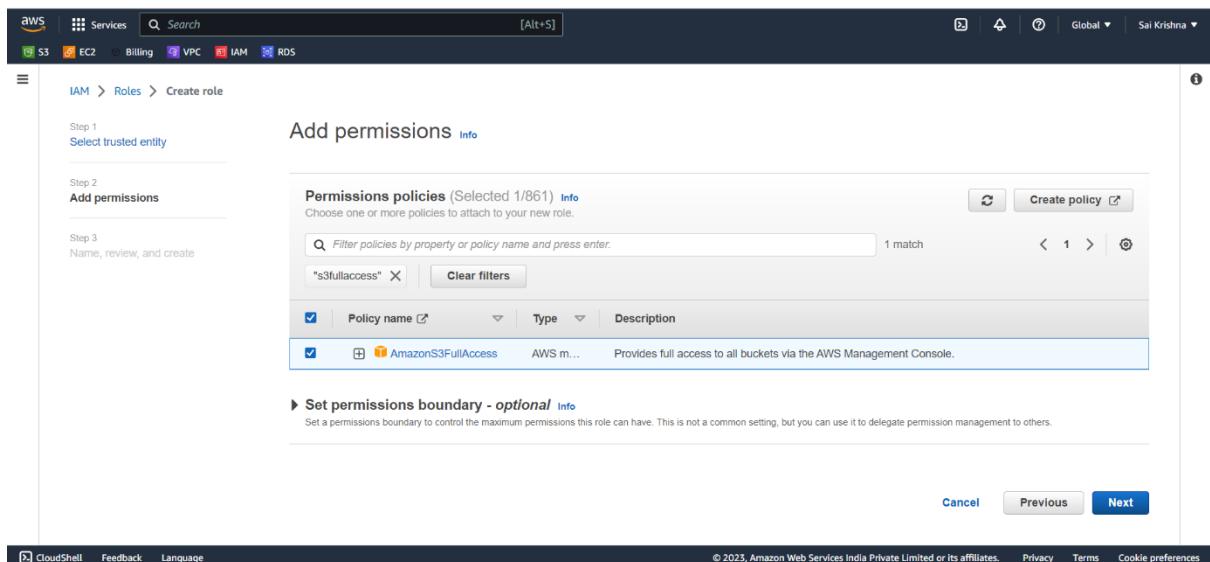


- In the Select type of trusted entity dialog box, select AWS service.

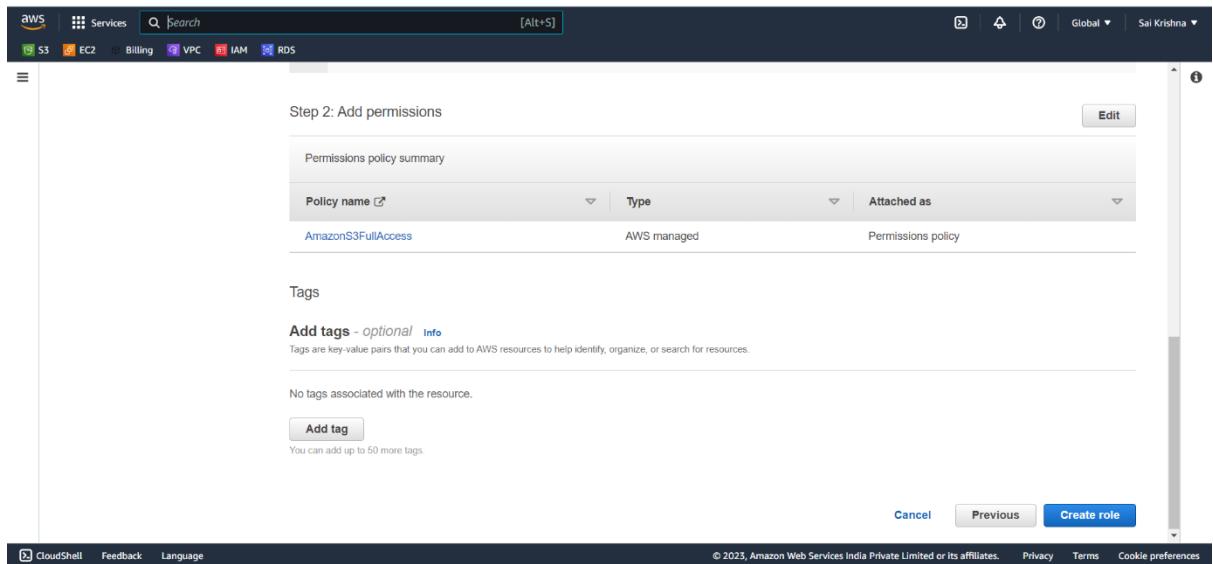
- In the Select service dialog box, select EC2.



- Click the Next: Permissions button.
- In the Attach permissions policies dialog box, search for the policy AmazonS3FullAccess and select it.



- Click the Next: Tags button.
- (Optional) In the Tags dialog box, add tags to your role.



- Click the Next: Review button.
- In the Review dialog box, review the settings for your role.
- Click the Create role button.

The screenshot shows the AWS IAM Roles page. A green success message at the top right says "Role calls3fromproject created." The main table lists eight roles, including the newly created one. The columns are "Role name", "Trusted entities", and "Last act...". The "calls3fromproject" role is listed under "AWS Service: ec2".

Role name	Trusted entities	Last act...
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	AWS Service: dynamodb.application-autoscaling (Service-Linked Role)	4 days ago
AWSServiceRoleForRDS	AWS Service: rds (Service-Linked Role)	2 hours ago
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
calls3fromproject	AWS Service: ec2	-
rds-monitoring-role	AWS Service: monitoring.rds	-
role_001	AWS Service: ec2	9 days ago
e3err_role_for_ec2ERR.com	AWS Service: e3	9 days ago

- Once the role has been created, you can verify that it was created successfully by checking the Roles page in the AWS Management Console.
- The role should be listed with the name calls3fromproject and the permissions policy AmazonS3FullAccess attached to it.
- In the EC2 dashboard, select the instance that you want to modify.
- In the Details pane, click the Security tab.

The screenshot shows the EC2 Instances page with the path "EC2 > Instances > i-0737de746e62598ca > Modify IAM role". The "Modify IAM role" dialog box is open, showing the "Instance ID" as "i-0737de746e62598ca (instance-01)". In the "IAM role" section, a dropdown menu shows "calls3fromproject" selected. Below the dropdown is a "Create new IAM role" button. At the bottom are "Cancel" and "Update IAM role" buttons.

- In the IAM role section, click the Modify button.
- In the Select IAM role dialog box, search for the role calls3fromproject and select it.
- Click the Save button.
- Once the role has been updated, you can verify that the calls3fromproject role has been attached to it by checking the IAM role section.

The screenshot shows the AWS EC2 Instances page. The top navigation bar includes the AWS logo, Services, a search bar, and account information for Mumbai and Sai Krishna. The left sidebar has sections for New EC2 Experience, EC2 Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images (AMIs, AMI Catalog), CloudShell, Feedback, and Language. The main content area displays a table titled 'Instances (1) Info' with one row for 'instance-01'. The instance details are: Name: instance-01, Instance ID: i-0737de746e62598ca, Instance state: Running (green checkmark), Instance type: t2.micro, Status check: 2/2 checks passed, Alarm status: No alarms, Availability Zone: ap-south-1a. A success message at the top says 'Successfully attached calls3fromproject to instance i-0737de746e62598ca'. Below the table is a section titled 'Select an instance'.

- Now connect to instance.

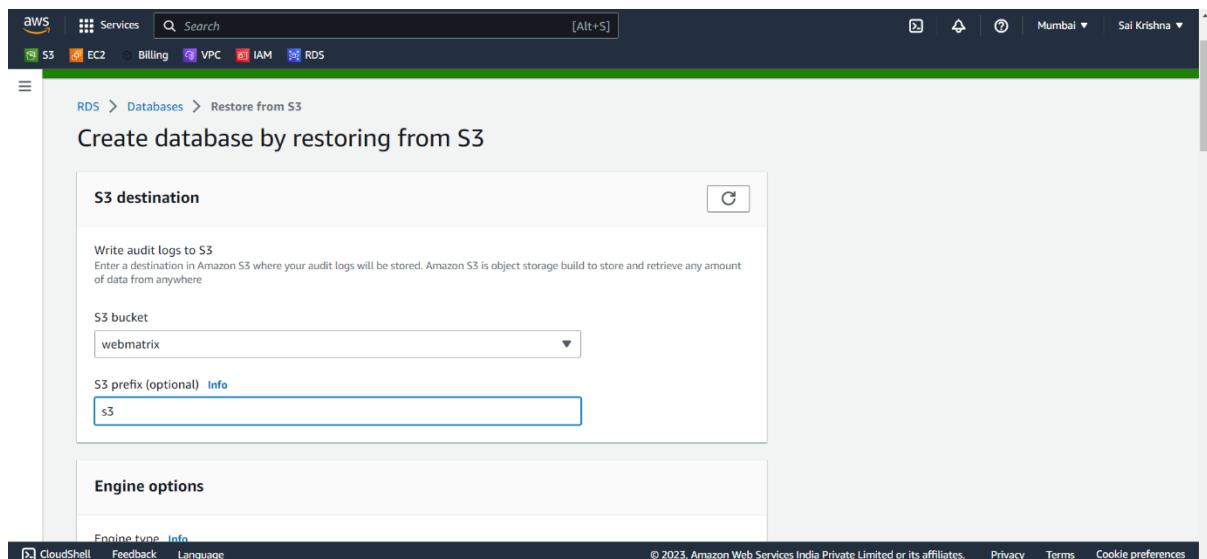
The screenshot shows the 'Connect to instance' dialog box for the instance i-0737de746e62598ca (instance-01). The top navigation bar and sidebar are identical to the previous screenshot. The dialog box has tabs for EC2 Instance Connect (selected), Session Manager, SSH client, and EC2 serial console. The 'EC2 Instance Connect' tab shows the instance ID and two connection options: 'Connect using EC2 Instance Connect' (selected, with a blue border) and 'Connect using EC2 Instance Connect Endpoint'. Below these are fields for Public IP address (3.109.185.50) and User name (ec2-user). A note at the bottom states: 'Note: In most cases, the default user name, ec2-user, is correct. However, read your AMI usage instructions to learn more about the user name.' The bottom of the dialog box includes CloudShell, Feedback, Language, and copyright information.

- Create file.txt with content of Roll , Number by using CLI as follows
 - cat > file.txt
 - Upload file.txt to S3 Bucket through CLI as follows
 - aws s3 cp file.txt s3://webmatrix

service 5:RDS

Steps to perform:

- In the AWS Management Console, click the RDS service.
- In the RDS dashboard, click the Databases tab.
- In the Actions menu, select Restore from S3.
- In the Restore from S3 dialog box, enter the following information:
 - S3 bucket: The name of the S3 bucket(webmatrix) that contains the file.txt.
 - IAM role: The IAM role that has permissions to access the S3 bucket.



- Click the Create database checkbox.
- Enter the following information for the new database:
 - Database name: The name of the new database is database-1.
 - Engine: The database engine that you want to use.
 - Version: The database engine version that you want to use.

The screenshot shows the 'Engine options' section of the AWS RDS console. At the top, there are two radio button options: 'Aurora (MySQL Compatible)' (selected) and 'MySQL'. Below each option is a small icon: a starburst for Aurora and a hand holding a database for MySQL. Underneath these, a section titled 'Available versions (14/15)' shows 'Aurora (MySQL 5.7) 2.11.2' with a dropdown arrow. On the right side of the screen, there's a sidebar with 'IAM role' settings, including a dropdown menu set to 'calls3fromproject'. The bottom of the page includes standard AWS navigation links like CloudShell, Feedback, Language, and footer copyright information.

- Instance class: The instance class that you want to use for the new database. Select Memory optimized classes from the Instance class drop-down list.
- Storage type: The storage type that you want to use for the new database.

The screenshot shows the 'Instance configuration' section of the AWS RDS console. It displays the DB instance configuration options for the selected engine. Under 'DB instance class', 'Memory optimized classes (includes r classes)' is selected. A dropdown menu shows 'db.r6g.2xlarge' as the chosen option, with details: 8 vCPUs, 64 GiB RAM, and Network: 4,750 Mbps. There is also a checkbox for 'Include previous generation classes' which is unchecked. Below this, the 'Settings' section is visible, containing fields for 'DB cluster identifier' (set to 'database-1') and a note about case-insensitivity and character constraints. The bottom of the page includes standard AWS navigation links and footer copyright information.

- Master password: The master password for the new database.
- Click the Restore button.

Auto generate a password Amazon RDS can generate a password for you, or you can specify your own password.

Master password [Info](#)

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), '(single quote)', "(double quote) and @ (at sign).

Confirm master password [Info](#)

Availability & durability

Multi-AZ deployment [Info](#)
 Create an Aurora Replica or Reader node in a different AZ (recommended for scaled availability)
Creates an Aurora Replica for fast failover and high availability.
 Don't create an Aurora Replica

Create database

- Once the restore operation has completed, the database will be restored from the S3 bucket and a new database will be created.

Introducing Aurora I/O-Optimized
Aurora's I/O-Optimized [\[\]](#) is a new cluster storage configuration that offers predictable pricing for all applications and improved price-performance, with up to 40% costs savings for I/O-intensive applications.

RDS > Databases

Databases (1)

DB identifier	Status	Role	Engine	Region & AZ	Size	Actions	CPU	Current activity
database-1	Available	Instance	MySQL Community	ap-south-1a	db.t2.micro	2 Actions	38.52%	0 Connections

<https://ap-south-1.console.aws.amazon.com/rds/home?region=ap-south-1#database;id=database-1;is-cluster=false>

- add inbound rules for security group in database-1.

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

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-09df471120d7f43d1	SSH	TCP	22	Anywhere (0.0.0.0/0)	
sgr-0dd53526da3805982	All traffic	All	All	Anywhere (0.0.0.0/0)	
-	MySQL/Aurora	TCP	3306	Anywhere (0.0.0.0/0)	

Add rule

Cancel | Preview changes | Save rules

- we can see the database using following command :

➤ **mysql -h endpoint -P 3306 -u admin -p**

- copy the endpoint from database-1.

Amazon RDS

Connectivity & security | Monitoring | Logs & events | Configuration | Maintenance & backups | Tags

Endpoint & port	Networking	Security
Endpoint database-1.ci8khoc4nrdu.ap-south-1.rds.amazonaws.com	Availability Zone ap-south-1a	VPC security groups sa_sg (sg-05cb066db1f35737c) Active
Port 3306	VPC vpc-01 (vpc-095db84d33c8b4249)	Publicly accessible No
	Subnet group default-vpc-095db84d33c8b4249	Certificate authority Info rds-ca-2019
	Subnets subnet-018fd94aa2ac9cb78 subnet-0cff2446763b33843	Certificate authority date August 22, 2024, 22:38 (UTC+05:30)

CloudShell | Feedback | Language

```
Last login: Mon Jul 24 05:45:33 2023 from ec2-13-233-177-5.ap-south-1.compute.amazonaws.com
[ec2-user@ip-10-0-0-40 ~]$ sudo su
[root@ip-10-0-0-40 ec2-user]# aws s3 ls
2023-07-24 03:55:55 webmatrix
[root@ip-10-0-0-40 ec2-user]# mysql -h database-1.ci8khoc4nrdu.ap-south-1.rds.amazonaws.com -P 3306 -u admin -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 41
Server version: 8.0.33 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
```

CloudShell | Feedback | Language

```

MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
| webmatrix |
+-----+
5 rows in set (0.00 sec)

MySQL [(none)]> use webmatrix;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [webmatrix]> show tables;
+-----+
| Tables_in_webmatrix |
+-----+
| mytable |
+-----+
1 row in set (0.00 sec)

MySQL [webmatrix]> select * from mytable;
+----+----+
| roll | number |
+----+----+
| 1   | 1       |
+----+----+
1 row in set (0.00 sec)

```

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

- In the RDS dashboard, click the Databases tab.
- In the list of databases, select the database-1 that you want to create a read replica for.
- In the Actions menu, select Create Read Replica.

Amazon RDS

- Dashboard
- Databases**
- Query Editor
- Performance insights
- Snapshots
- Exports in Amazon S3
- Automated backups
- Reserved instances
- Proxies

Subnet groups

Parameter groups

Option groups

Custom engine versions

RDS > Databases

Introducing Aurora I/O-Optimized

Aurora's I/O-Optimized is a new cluster storage configuration that offers predictable pricing and up to 40% costs savings for I/O-intensive applications.

Consider creating a Blue/Green Deployment to minimize downtime during upgrades. You may want to consider using Amazon RDS Blue/Green Deployments and minimize downtime by creating a copy of your production database in a different environment. RDS User Guide

Databases (1)

DB identifier	Status	Role	Engine	Region & AZ	Size	Actions	CPU
database-1	Available	Instance	MySQL Community	ap-south-1a	db.t2.micro	2 Actions	I 3.7

Actions ▾ Restore from S3 Create database

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

- In the Create Read Replica dialog box, enter the following information:

The screenshot shows the 'Create read replica' dialog box in the AWS RDS console. The 'Settings' tab is active. Under 'Replica source', the 'Source DB instance identifier' dropdown is set to 'database-1'. The 'DB instance identifier' input field is empty. Below these fields, there is a note about the DB instance identifier being a unique key for a DB instance. The 'Instance configuration' tab is also visible.

- DB instance identifier: The name of the read replica is database.
- DB instance class: The instance class that you want to use for the read replica.

The screenshot shows the 'Instance configuration' section of the AWS RDS console. Under 'DB instance class', 'Burstable classes (includes t classes)' is selected, with 'db.t2.micro' chosen. Below it, 'Include previous generation classes' is checked. In the 'AWS Region' section, 'Destination Region' is set to 'Asia Pacific (Singapore)'. The bottom navigation bar includes CloudShell, Feedback, Language, and links for Privacy, Terms, and Cookie preferences.

- Storage type: The storage type that you want to use for the read replica.
- Region: The region where you want to create the read replica.

The screenshot shows the 'Storage' configuration section. 'Storage type' is set to 'General Purpose SSD (gp2)'. 'Allocated storage' is set to 20 GiB. A note indicates that provisioning less than 100 GiB could result in higher latencies. 'Enable storage autoscaling' is checked. The bottom navigation bar includes CloudShell, Feedback, Language, and links for Privacy, Terms, and Cookie preferences.

- Multi-AZ deployment: Whether you want to create a Multi-AZ read replica.

Storage autoscaling [Info](#)

Provides dynamic scaling support for your database's storage based on your application's needs.

Enable storage autoscaling
Enabling this feature will allow the storage to increase after the specified threshold is exceeded.

Maximum storage threshold [Info](#)
Charges will apply when your database autoscales to the specified threshold

22 [GiB](#)

The minimum value is 22 GiB and the maximum value is 6,144 GiB

Availability

Deployment options [Info](#)
The following deployment options are limited to those supported by the engine.

- Multi-AZ DB Cluster - new**
Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.
- Multi-AZ DB instance**
Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.
- Single DB instance**
Creates a writer DB instance with no reader DB instances.

- Click the Create button.

Connectivity

Network type [Info](#)
To use dual-stack mode, make sure that you associate an IPv6 CIDR block with a subnet in the VPC you specify.

- IPv4**
Your resources can communicate only over the IPv4 addressing protocol.
- Dual-stack mode**
Your resources can communicate over IPv4, IPv6, or both.

DB subnet group [Info](#)
Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.

None

Public access

- Publicly accessible**
RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.
- Not publicly accessible**
No IP address is assigned to the DB instance. EC2 instances and devices outside the VPC can't connect.

- Once the read replica has been created, it will be available in the Singapore region.

Databases (1)

DB identifier	Status	Role	Engine	Region & AZ	Size	Actions	CPU	Current activity
database	Creating	Replica	MySQL Community	-	db.t2.micro	-	-	-

Creating an EC2 instance in Singapore region:

- Name your instance as instance-02,
- Select “amazon linux 2 ami (hvm) - kernel 5.10 ssd volume type”.

Number of instances: 1

Software Image (AMI): Amazon Linux 2 Kernel 5.10 AMI...
ami-09964535fc01efa5f

Virtual server type (instance type): t2.micro

Firewall (security group): sai_01

Storage (volumes): 1 volume(s) - 8 GiB

Free tier: In your first year

Launch instance

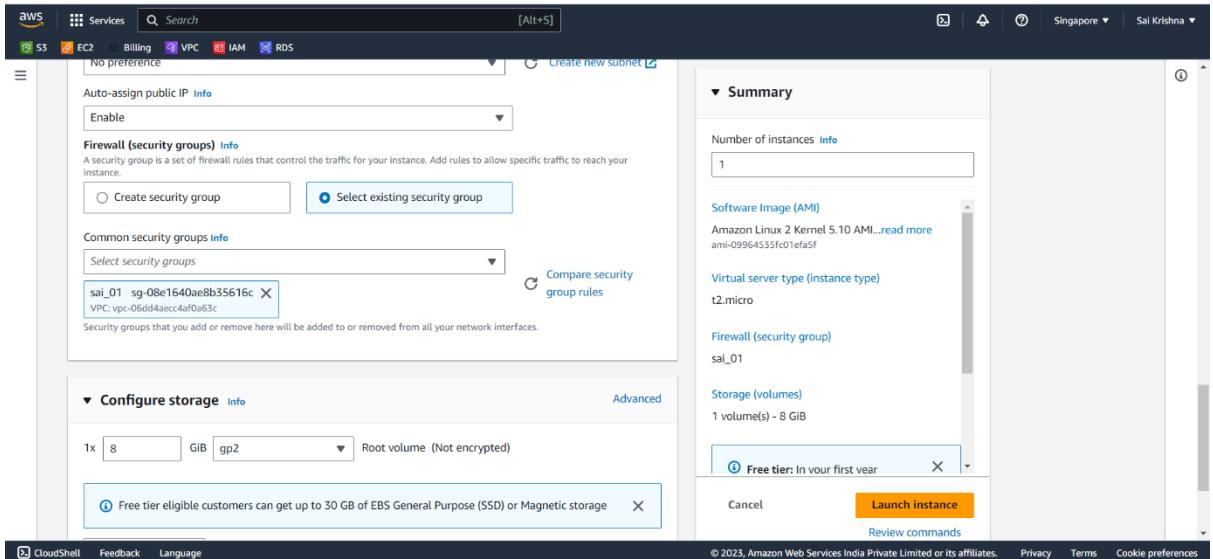
- Instance type “t2. micro”.

The screenshot shows the AWS Quick Start interface for launching a new instance. The selected AMI is "Amazon Linux 2 AMI (HVM - Kernel 5.10, SSD Volume Type)" with the ID "ami-09964535fc01efa5f". The instance type is set to "t2.micro". Other visible settings include a security group named "sai_01" and a volume of 8 GiB. A "Launch instance" button is at the bottom right.

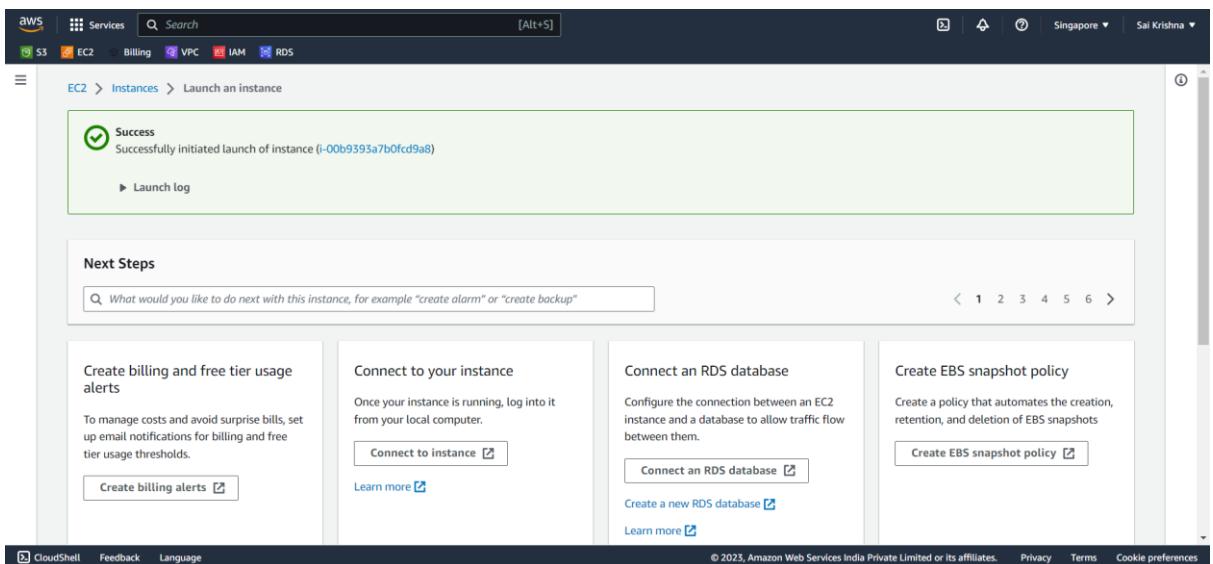
- Select your existing key pair.

The screenshot shows the AWS Launch Instance wizard. The current step is "Key pair (login)", where the user has selected the key pair "sai_sing". Previous steps shown are "Instance type" (set to t2.micro) and "Network settings" (VPC: vpc-06dd4aecc4af0a63c, Subnet: default). The "Launch instance" button is visible at the bottom.

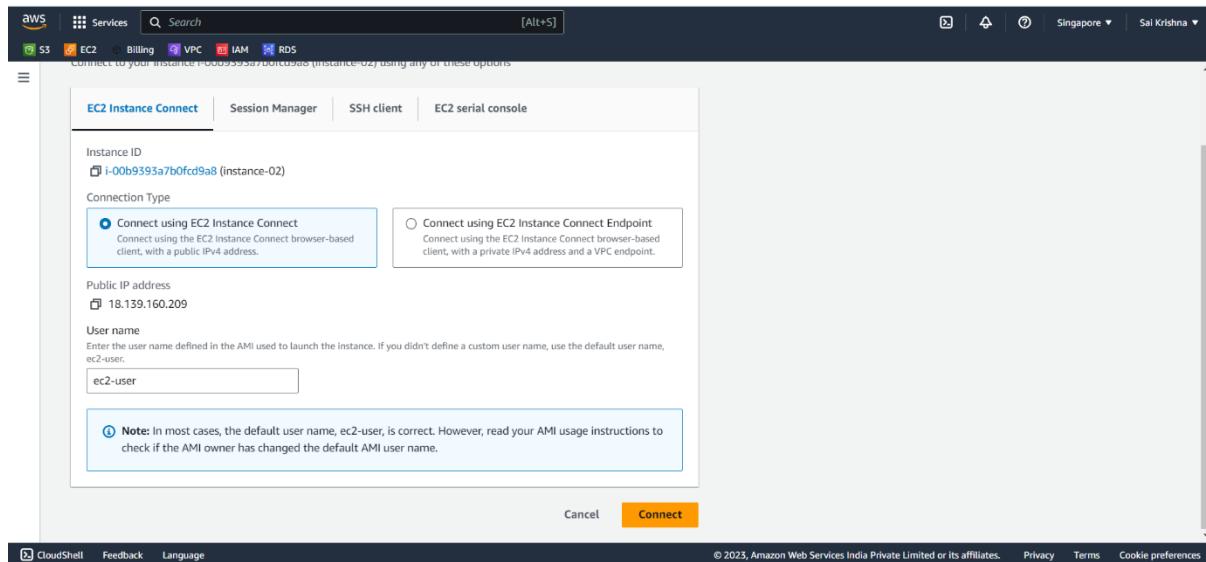
- Select your default VPC.
- In the security group section, select availability zone as southeast-1a.
- create a new security group, add security groups that supports SSH and all the traffic.



- Launch your instance in Singapore region.



- Now connect the instance-02.



```

AWS | Services | Search [Alt+S]
S3 EC2 Billing VPC IAM RDS
Last login: Mon Jul 24 06:10:56 2023 from ec2-3-0-5-37.ap-southeast-1.compute.amazonaws.com
[ec2-user@ip-172-31-44-166 ~] 
[ec2-user@ip-172-31-44-166 ~] / Amazon Linux 2 AMI
[ec2-user@ip-172-31-44-166 ~] 

https://aws.amazon.com/amazon-linux-2/
7 package(s) needed for security, out of 7 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-44-166 ~]$ sudo yum install mysql
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
Package 1:mariadb-5.6.8-1.amzn2.0.1.x86_64 already installed and latest version
Nothing to do
[ec2-user@ip-172-31-44-166 ~]$ mysql -h database.csm3kr923r0u.ap-southeast-1.rds.amazonaws.com -P 3306 -u admin -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 33
Server version: 8.0.33 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;

i-07a773ab49ddbbc28 (instance-02)
PublicIPs: 13.212.31.239 PrivateIPs: 172.31.44.166

```

```

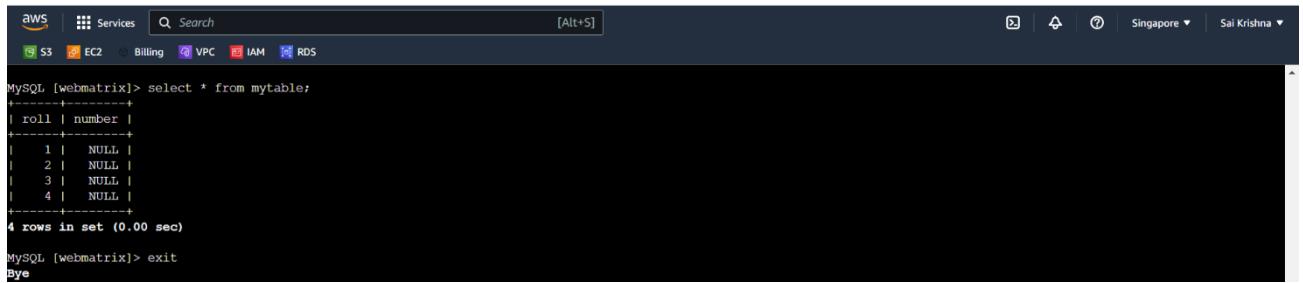
AWS | Services | Search [Alt+S]
S3 EC2 Billing VPC IAM RDS
MySQL [(none)]> show databases;
+-----+
| Database      |
+-----+
| information_schema |
| mysql          |
| performance_schema |
| sys            |
| webmatrix      |
+-----+
5 rows in set (0.00 sec)

MySQL [(none)]> use webmatrix;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL {webmatrix}> show tables;
+-----+
| Tables_in_webmatrix |
+-----+
| mytable           |
+-----+
1 row in set (0.01 sec)

i-07a773ab49ddbbc28 (instance-02)
PublicIPs: 13.212.31.239 PrivateIPs: 172.31.44.166

```



A screenshot of the AWS Management Console interface. At the top, there's a navigation bar with the AWS logo, a 'Services' dropdown, a search bar, and user information for 'Sai Krishna'. Below the navigation bar, the 'RDS' service is selected from a horizontal menu. The main area shows a MySQL terminal window. The terminal output is as follows:

```
MySQL [webmatrix]> select * from mytable;
+----+-----+
| roll | number |
+----+-----+
| 1   | NULL  |
| 2   | NULL  |
| 3   | NULL  |
| 4   | NULL  |
+----+
4 rows in set (0.00 sec)

MySQL [webmatrix]> exit
Bye
```

Conclusion:

In conclusion, the data flow from EC2 to S3 and then from S3 to RDS (database) and then from that RDS (database) to another RDS (database) using read replica and we can see data from that EC2 connect is a scalable, secure, and flexible data pipeline. It can be used to process a variety of data types, and it can be scaled to handle large volumes of data. The data is stored in S3 and RDS, which are both secure services. The data can be accessed from multiple EC2 instances, which allows for flexibility in how the data is used.

The data flow is a good example of how AWS services can be used to build scalable, secure, and flexible data pipelines. It can be used by a variety of organizations, including businesses, government agencies, and educational institutions.