AWS (AMAZON WEB SERVICES)
Simple Storage Service(S3) and SNS

SIMPLE STORAGE SERVICE:

Amazon Simple Storage Service is storage for the Internet. It is designed to make web-scale computing easier for developers.

Amazon S3 has a simple web services interface that you can use to store and retrieve any amount of data, at any time, from anywhere on the web. It gives any developer access to the same highly scalable, reliable, fast, inexpensive data storage infrastructure that Amazon uses to run its own global network of websites.

Characteristics of S3:

1. S3 is the object level storage.
2. In S3 you can't install any softwares, but in EBS volumes we can.
3. In S3 objects are stored as Key and Values.
4. In S3 size of each object can be upto 5 TB.
5. S3 supports server side encryption at rest.
6. By using S3 we can host static websites.
7. S3 supports REST API and SOAP APIs.
8. S3 can be extendable upto very high, and you can store unlimited data.
9. In S3 no need to specify any size.
10. S3 is highly durable (S3 maintains 3 replicas across 3 AZs).
11. S3 is region specific.

Use Cases of S3:

1. Backups and recovery.
2. Big data analytics.
3. Storage artifacts(Jar/war/ear).
4. We can also store application logs.
5. We can also store audios, videos, excel files, word documents, text files etc..
6. Disaster recovery.

Components of S3:

S3 Bucket: To upload your data (photos, videos, documents etc.), you first create a bucket in one of the AWS Regions. You can then upload any number of objects to the bucket.

S3 Objects: Objects is the fundamental entities stored in S3 buckets.

Keys: A key is unique identifier for an object within a bucket. Every object in a bucket has exactly one key.

S3 storage classes:

1. General Purpose
2. Infrequent Access
3. Archive

1. General Purpose:

Amazon S3 Standard: Amazon S3 Standard offers high durability, availability, and performance object storage for frequently accessed data.
Features:

1. Low latency and high throughput performance
2. Designed for durability of 99.999999999% of objects across multiple Availability Zones
3. Data is resilient in the event of one entire Availability Zone destruction
4. Designed for 99.99% availability over a given year.
5. Supports SSL for data in transit and encryption of data at rest.
6. Lifecycle management for automatic migration of objects.

2. Infrequent Access:

i) Amazon S3 Standard-Infrequent Access:

Amazon S3 Standard-Infrequent Access (S3 Standard-IA) is an Amazon S3 storage class for data that is accessed less frequently, but requires rapid access when needed. S3 Standard-IA offers the high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee. This combination of low cost and high performance make S3 Standard-IA ideal for long-term storage, backups, and as a data store for disaster recovery.

Features:

1. Same low latency and high throughput performance of S3 Standard
2. Designed for durability of 99.999999999% of objects across multiple Availability Zones
3. Data is resilient in the event of one entire Availability Zone destruction
4. Designed for 99.9% availability over a given year
5. Supports SSL for data in transit and encryption of data at rest
6. Lifecycle management for automatic migration of objects

ii) Amazon S3 One Zone-Infrequent Access

Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) is an Amazon S3 storage class for data that is accessed less frequently, but requires rapid access when needed. Unlike other Amazon object storage classes, which store data in a minimum of three

AWS (AMAZON WEB SERVICES)
Simple Storage Service(S3) and SNS

Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ. Because of this, storing data in S3 One Zone-IA costs 20% less than storing it in S3 Standard-IA.
Features:

1. Same low latency and high throughput performance of S3 Standard and S3 Standard-IA
2. Designed for durability of 99.999999999% of objects in a single Availability Zone, but data will be lost in the event of Availability Zone destruction
3. Designed for 99.5% availability over a given year.
4. Supports SSL for data in transit and encryption of data at rest
5. Lifecycle management for automatic migration of objects.

3. Archive: *Amazon Glacier:* Amazon Glacier is a secure, durable, and extremely low-cost storage service for data archiving. You can reliably store any amount of data at costs that are competitive with or cheaper than on-premises solutions. *Key Features:*

1. Designed for durability of 99.999999999% of objects across multiple Availability Zones
2. Data is resilient in the event of one entire Availability Zone destruction
3. Supports SSL for data in transit and encryption of data at rest
4. Extremely low cost design is ideal for long-term archive
5. Lifecycle management for automatic migration of objects.

	S3 Standard	S3 Standard-IA	S3 One Zone-IA	Amazon Glacier
Designed for Durability	99.999999999%	99.999999999%	99.999999999%†	99.999999999%
Designed for Availability	99.99%	99.9%	99.5%	N/A
Availability SLA	99.9%	99%	99%	N/A
Availability Zones	≥3	≥3	1	≥3
Minimum Capacity Charge per Object	N/A	128KB*	128KB*	N/A
Minimum Storage Duration Charge	N/A	30 days	30 days	90 days
Retrieval Fee	N/A	per GB retrieved	per GB retrieved	per GB retrieved**
First Byte Latency	milliseconds	milliseconds	milliseconds	select minutes or hours***
Storage Type	Object	Object	Object	Object
Lifecycle Transitions	Yes	Yes	Yes	Yes

Address: *MP Techno Solutions*, Above Titan ShowRoom, Marathahalli, Bangalore, Phone: 9606955170/1/2/3

S3 Versioning:

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.

Features of Versioning:

1. If you delete an object, instead of removing it permanently, Amazon S3 inserts a delete marker, which becomes the current object version. You can always restore the previous version.
2. If you overwrite an object, it results in a new object version in the bucket. You can always restore the previous version.

Note: Once you version-enable a bucket, it can never return to an unversioned state. You can, however, suspend versioning on that bucket.

Implementation:

Select Bucket → Properties → Enable Versioning → Save

S3 Server access logging:

1. Server access logging provides detailed records for the requests that are made to a bucket. Server access logs are useful for many applications. For example, access log information can be useful in security and access audits. It can also help you learn about your customer base and understand your Amazon S3 bill.
2. Simply we can say S3 Server access logging keeps the records of all API activities.
3. To track requests for access to your bucket, you can enable server access logging. Each access log record provides details about a single access request, such as the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Note:

1. There is no extra charge for enabling server access logging on an Amazon S3 bucket.
2. However, any log files that the system delivers to you accrue the usual charges for storage.
3. No data transfer charges are assessed for log file delivery, but access to the delivered log files is charged the same as any other data transfer.
4. By default, logging is disabled. When logging is enabled, logs are saved to a bucket in the same AWS Region as the source bucket.

Implementation:

Select Bucket → Properties → Server Access Logging → Select Target Bucket → Select Prefix folder of the Bucket → Save

S3 Events:

The Amazon S3 notification feature enables you to receive notifications when certain events happen in your bucket. To enable notifications, you must first add a notification configuration identifying the events you want Amazon S3 to publish, and the destinations where you want Amazon S3 to send the event notifications.

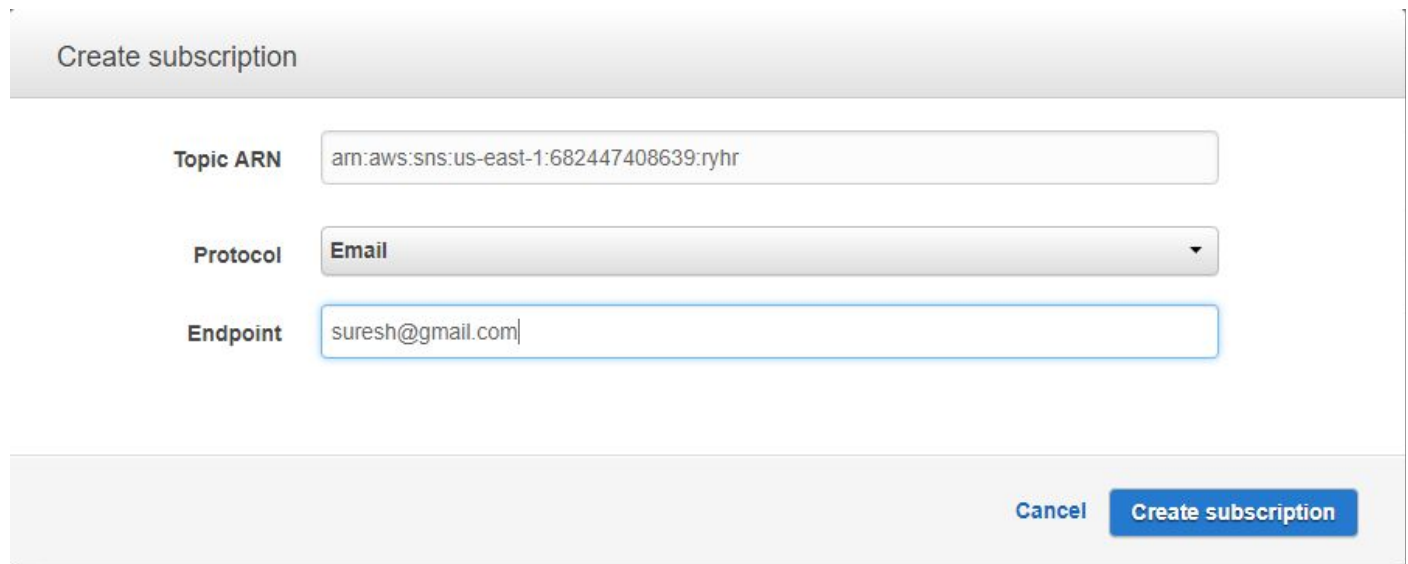**Amazon S3 Events supports the following destinations where it can publish events:**

1. SNS(Simple Notification Service) Topic
2. SQS (Simple Queue Service)
3. Lambda

S3 Events for SNS Topic:

Implementation:

1. *From SNS Dashboard → Topics → Create New Topic → Select Topic Name → Display Name → Create Topic*
2. *Select the Topic → Actions → Subscribe to Topic → In Protocol Select "Email" → Select "End Point" → Create Subscription*

Ex:

AWS VPC Endpoint for S3:

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by Private Link without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service.

There are two types of VPC endpoints:

1. Interface endpoints
2. Gateway endpoints.

Interface Endpoints (Powered by AWS Private Link):

An interface endpoint is an elastic network interface with a private IP address that serves as an entry point for traffic destined to a supported service. The following services are supported:

Amazon CloudWatch, Cloudwatch Logs, Cloudwatch Events, AWS EC2, SNS, Elastic Load Balancing API etc…
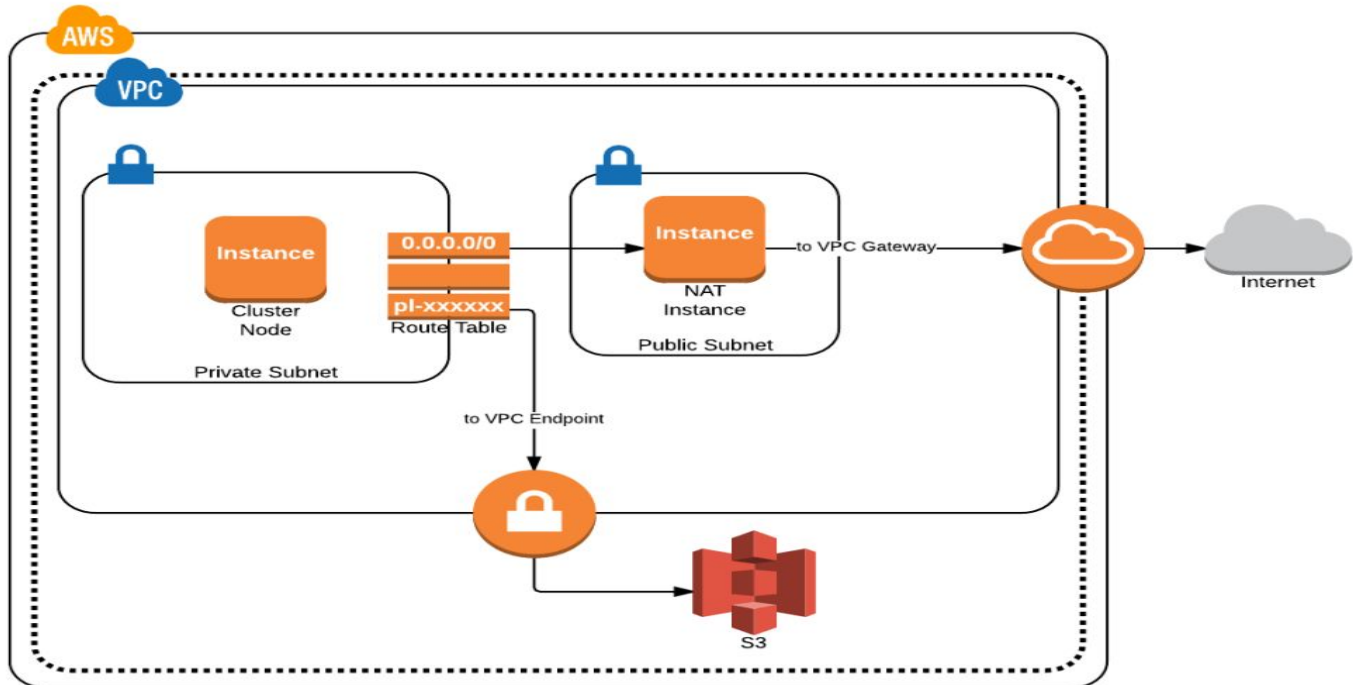
Gateway Endpoints:

A gateway endpoint is a gateway that is a target for a specified route in your route table, used for traffic destined to a supported AWS service. The following AWS services are supported:

- Amazon S3
- DynamoDB

Implementation:

AWS (AMAZON WEB SERVICES)
Simple Storage Service(S3) and SNS

1. First you create one VPC and two subnets, out of which one is Public another one is Private Subnet.
2. Launch two instances one in Public Subnet and another one in Private Subnet.
3. Now our aim is we want to access s3 buckets from that Private Instance which don't have internet or Public IP.
4. For that we want to create VPC Endpoints for that Private Subnet.
   VPC Dashboard → Endpoints → Create Endpoints → Select Service Category as "AWS Services" → Service Name as "com.amazonaws.us-west-2.s3"→ Select Your VPC and Private Subnet → In Policy give Full Access → Create Endpoint

Note:
1. No need to edit the route table of Private Route Table, it automatically create the route table for the Private Subnet.
2. Your VPC and your S3 buckets are in same region only, otherwise it will not works.
3. For Private Instance to access the S3 buckets you must give the permissions to the Private Instance on over S3 buckets.
   IAM → Roles → Create Role for EC2→ Permissions(S3 FULL ACCESS) → Name the Role → Create Role → Select Private Instance → Actions → Attach and replace IAM Role → Select Role → Attach.
4. VPC EndPoints only give private access to the S3, but it doesn't give S3 privileges.