AWS SERVICES
AWS Concepts

1. VPC (Virtual Private Cloud)

Size of a vpc

Using ip address range.

The aws devops engineer will split and allocate the ip address ranges for all the sub projects. This process is called subnet.

Subnet segmented part of a larger network

we define the size of vpc for a whole project with a ip address range(i.e how many ip addresses we need). The devops engineer splitting this ip address range for sub projects is sunbets.

Private subnets dont have access to internet.

Public subnet is the one that the user first access in a VPC.

Public subnet connect to internet

Using the internet gateway.

How do requests know where to go

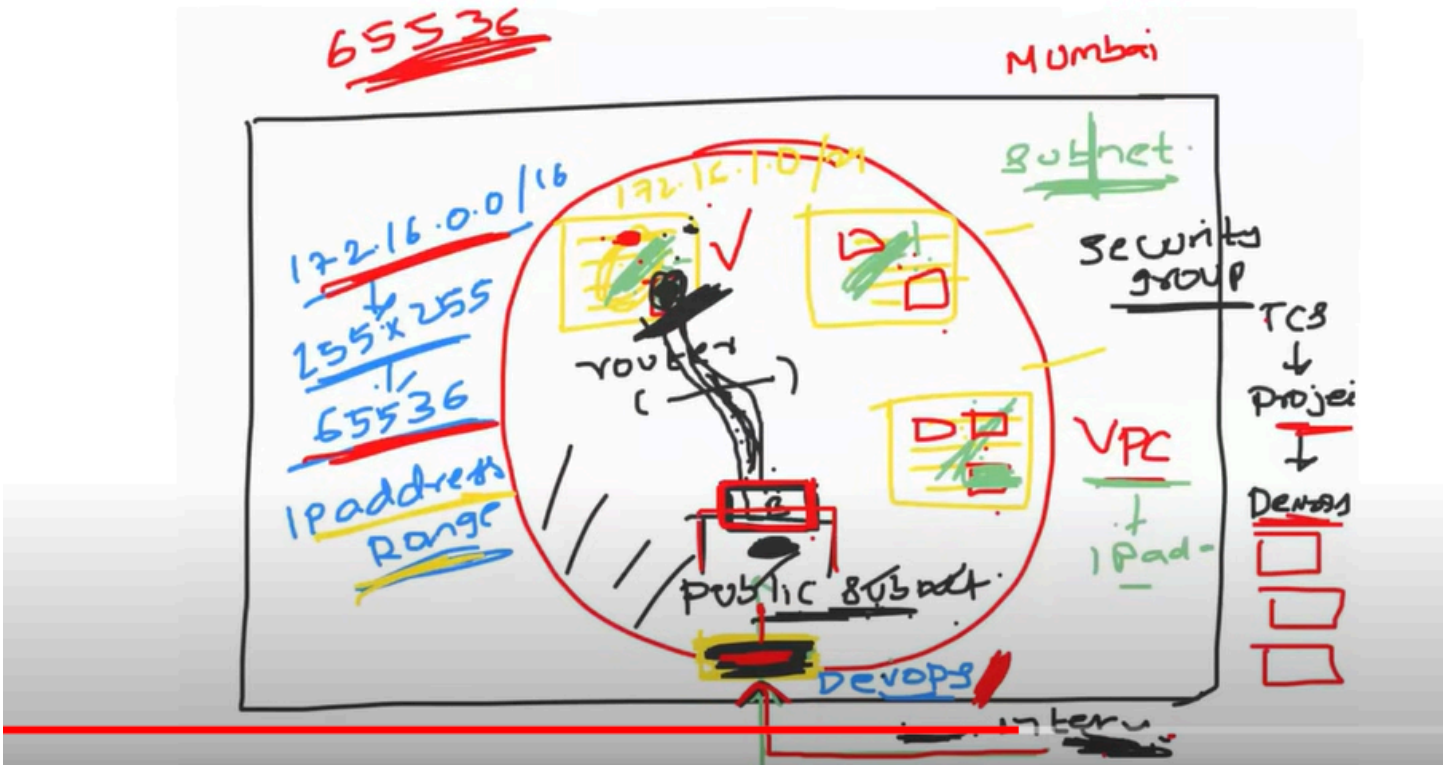
In a **public subnet**, there can be a **load balancer** (such as an AWS Elastic Load Balancer), which distributes incoming requests to the appropriate backend servers or services. You define **routing rules** (often in a route table) to direct traffic from the public subnet to the right destination, which can be resources in the private subnet or other instances in the VPC.

Scenario

Lets say with load balancer and route table the request is suppose to reach a ec2 instance in a private subnet. Will it reach the ec2 instance directly?

No. It cannot reach directly it should pass through the security group to reach the particular ec2 instance. It acts as a security check.

Flow diagram



What if the service in the private subnet needs to access the internet for some purpose eg:downloading someting from google ?

In such cases we should not expose the ip address of the private subnet to the end provider(i.e. google in this case)

Follow up : How do you avoid that ?

We should do masking of the ip address. This is addressed as NAT Gateways.

If this is acheived with load balancer we call it as SNAT.

If this is acheived with router we call it as Nat Gateway.

Security groups and nacl :

if we add security at the subnet level we call it NACL

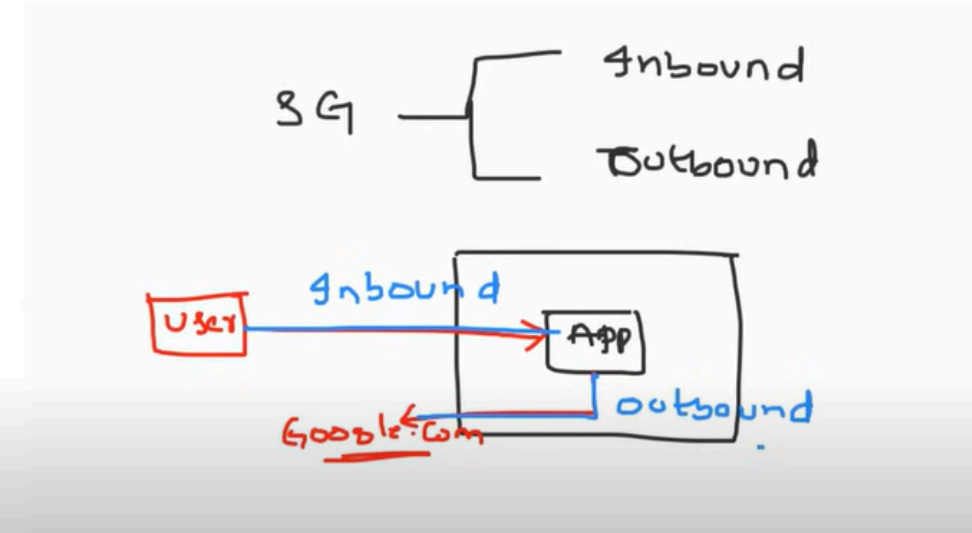
if we add security at the service leve i.e ec2 instance in a subnet level , we call it security groups.

these are last level security in vpc , hence leverage more importance.

More about Security Groups

2 things to look forward

- inbound traffic
- outbound traffic



AWS attach a security group by default , whill will allow all the outbound traffic except port 25 , and deny all the inbound traffic by default.

port 25 :

port 25 is a mailing service , aws by default not want to allow it.

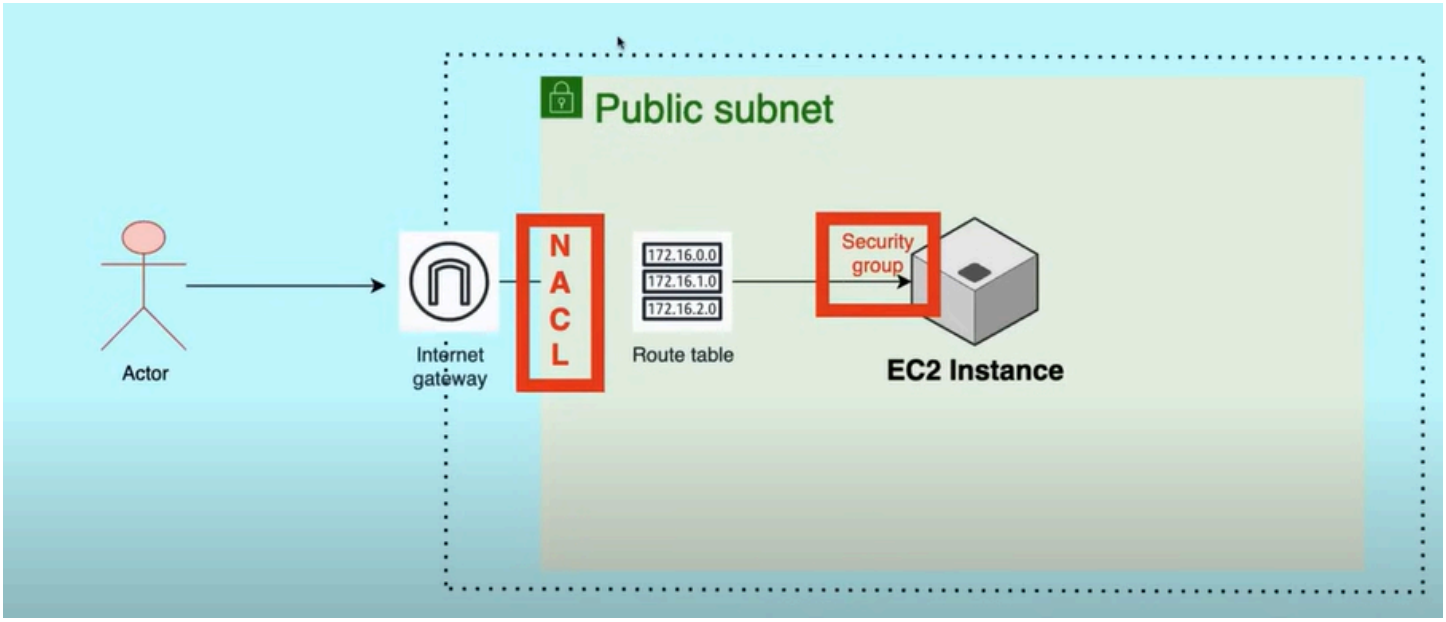
If security group does all these , they why do we need NACL ?

NACL → Network Access Control List

This is applied at the subnet level.

Scenario : Let's say we have 10,000 ec2 instances in a private subnet that needs similar security. So instead of adding 10,000 security groups one for each instance , we can add a nacl the that subnet itself.

1:



1. Explore VPC service
2. Create VPC (vpc and more option)
3. Create a ec2 instance and attach the above vpc

Login to the ec2 instance using git bash

update the instance // sudo yum update -y

1.cd /c/Users/018019/Downloads

2.chmod 400 aws.pem

3.ssh -i "aws.pem" ec2-user@your-public-ip

we will be logged in to the ec2 instance

4.start a http server at port 8000 // python3 -m http.server 8000

5.try to access it http://44.208.32.200:8000 → we can't access

Reason : At Nacl (subnet level → by default it allows incoming traffic) but in the default security group attached to instance , it denys incoming traffic.

6.Go to security groups → add rule to allow port 8000

now we can access it successfully.

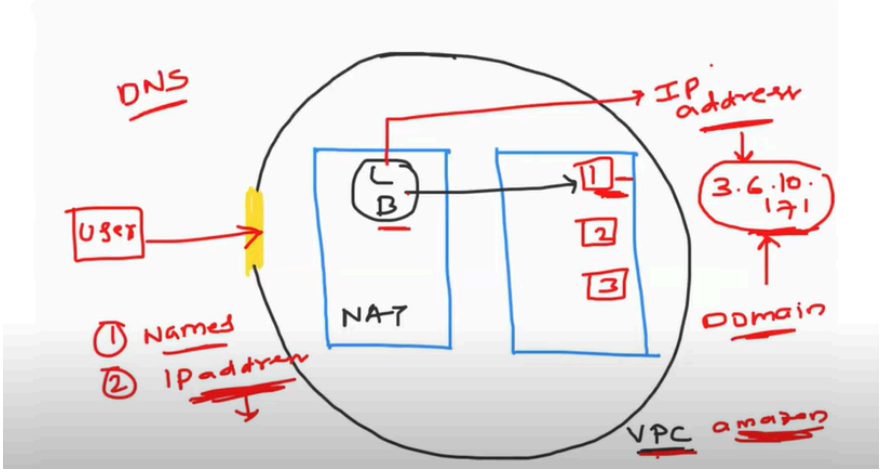
Note: In NACL , rule no matters , if we give allow 8000 on rule no 100, and deny 8000 on rule no 200 , then allow will only happen as 100 is taken as priority(i.e. ascending order)

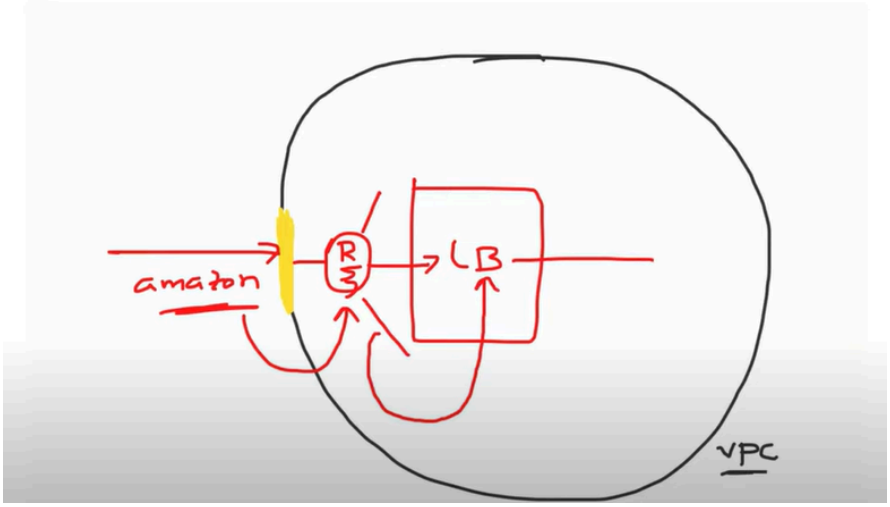
Route 53

Route 53 provides DNS as a service.

DNS → Domain Name System

DNS service maps/resolves the domain names to the corresponding ip addresses





route 53 will resolve the domain name and provide the ip address to be accessed to the Load Balancer

Example:

- You have a domain www.myapp.com.
- This domain is managed by Route 53, and you have configured it to route traffic to an **Elastic Load Balancer (ELB)**.
- When a user accesses www.myapp.com, Route 53 resolves it to the load balancer's DNS name (or IP address, depending on the setup).
- The load balancer then forwards the traffic to the appropriate backend resources (like EC2 instances) based on its configuration.

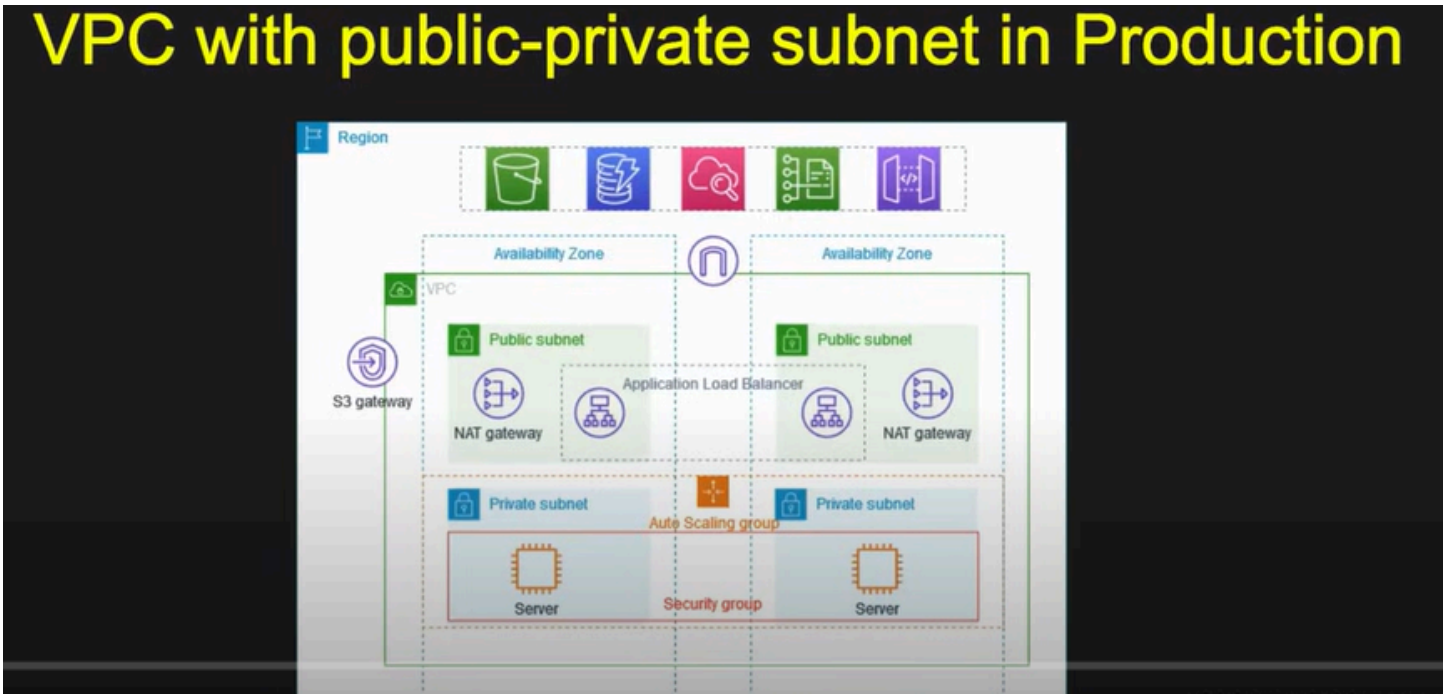
Route 53 steps involved :

1.Domain Registration

2.Hosted Zones (here we basically have the dns records)

Route 53 also supports Health Checks

2



Nat gateway

It enables instances in a private subnet to connect to internet or other aws services, while preventing those external connections accessing those private instances.

ASG

An **Auto Scaling Group (ASG)** in AWS is a service that automatically adjusts the number of Amazon EC2 instances in your application based on demand.

Bastion Host (also known as a **Jump Host**)

It acts as a secure gateway between the private subnet and public subnet , i.e. we cannot create a public ip to acces the instance in the private subnet , to resolve this we create a jump host in the public subnet , that will have the public ip , through which we can access the instance in the private subnet.

AWS S3

S3 stands for Simple Storage Service

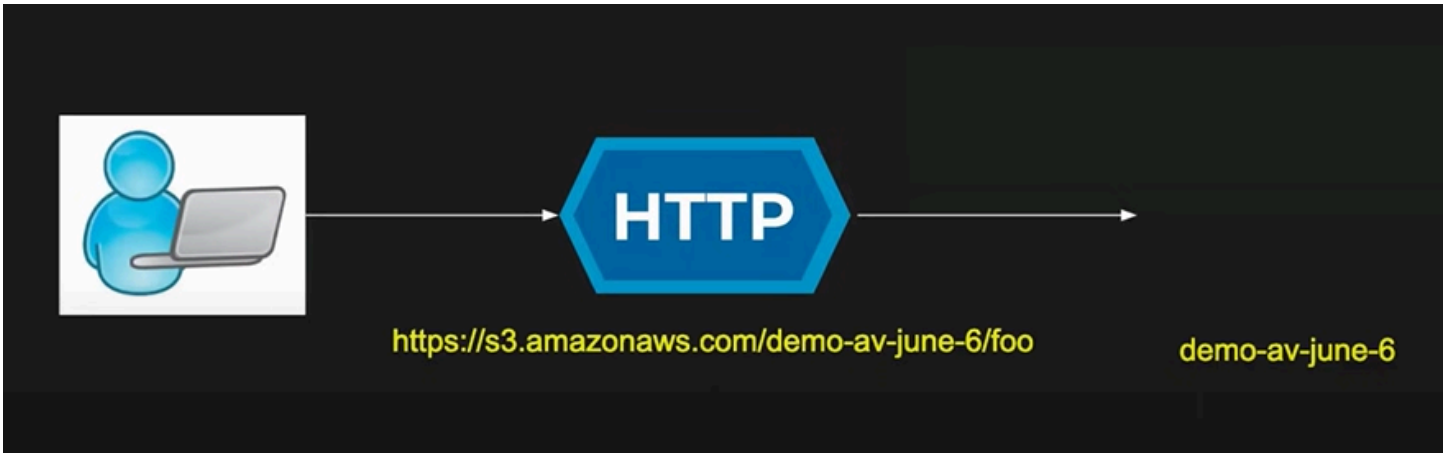
It is a storage service provided by amazon.

Scalable, High availability, secure, cost effective

S3 Buckets

S3 service allows us to create buckets and store anything. No restrictions.

Anything we upload in a s3 buckect , we can access it with a http protocol.



Hence objects in s3 becomes globally accessible. (Hence name of bucket should be unique globally)

Durability & Availability:

- S3 offers **99.999999999% (11 nines) durability** for objects stored, ensuring high data reliability.

- Data is automatically replicated across multiple geographically separated availability zones.

Benefits and Advantages of S3

- Avaiability and Durability
- Scalable (upto 5 tb)
- Secure (bucket policies, access contron , encryption settings)
- Cost Effective (but depends on the storage class)
- Performance (multiple regions support → latency) , Multipart uploads(uploading in chunks)

Storage Classes in S3?

Feature	S3 Standard	S3 Standard-IA	One Zone-IA	S3 Glacier	S3 Glacier Instant Retrieval	S3 Glacier Flexible Retrieval	S3 Glacier Deep Archive	S3 Outposts	S3 Intelligent-Tiering
Cost per GB per month	$0.02	$0.01	$0.01	$0.00	$0.00	$0.00	$0.00	$0.03	$0.015–0.025
Access time	1-15 seconds	3-5 minutes	3-5 minutes	12-48 hours	1-5 minutes	1-5 minutes	12-48 hours	Varies	Varies
Durability	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
Availability	99.90%	99.90%	99.90%	99.90%	99.90%	99.90%	99.90%	99.90%	99.90%
Minimum storage duration	Varies	Varies	Varies	Varies	Varies	Varies	Varies	Varies	Varies

Version Control in AWS S3

Amazon S3 supports **versioning**, which allows you to maintain multiple versions of an object within a bucket.

When versioning is enabled in an S3 bucket:

- Each time you upload an object with the same key (name), a new version is created.
- Older versions of the object are not overwritten but instead kept as distinct versions.
- Each version of an object is assigned a unique **version ID**.

If versioning is not enabled , then if we upload the same object then it will get overwritten.

AWS S3 access logging

Amazon S3 Access Logging is a feature that allows you to record detailed information about requests made to an S3 bucket.

Why Use S3 Access Logging?

- **Security Auditing**: Track who is accessing your buckets and objects, helping you identify unauthorized access or suspicious activities.
- **Performance Monitoring**: Understand traffic patterns, such as the number of requests and the types of operations performed (GET, PUT, DELETE, etc.).

- **Troubleshooting**: Diagnose issues by checking the status codes and the details of requests.

What is object lock in S3

Amazon S3 Object Lock is a feature that enables you to **prevent objects from being deleted or overwritten** for a specified period or indefinitely. This is particularly useful for scenarios that require **immutability**, such as compliance with legal and regulatory standards (e.g., WORM — Write Once, Read Many requirements).

Retention Period :

Governance Mode:

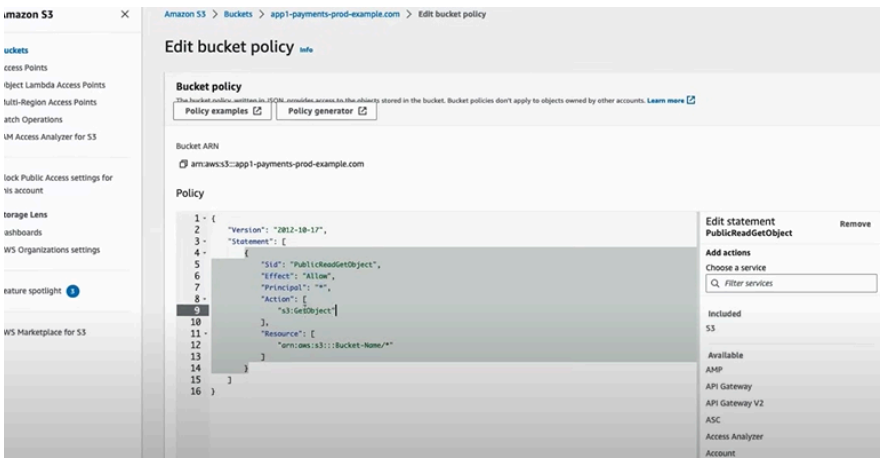
- Used in a media company where archives need to be protected for 3 years, but administrators should have the flexibility to update or delete archives in special cases with the right permissions.

Compliance Mode:

- Used by a financial institution storing transaction records that cannot be modified or deleted for a period of 7 years due to legal regulations.

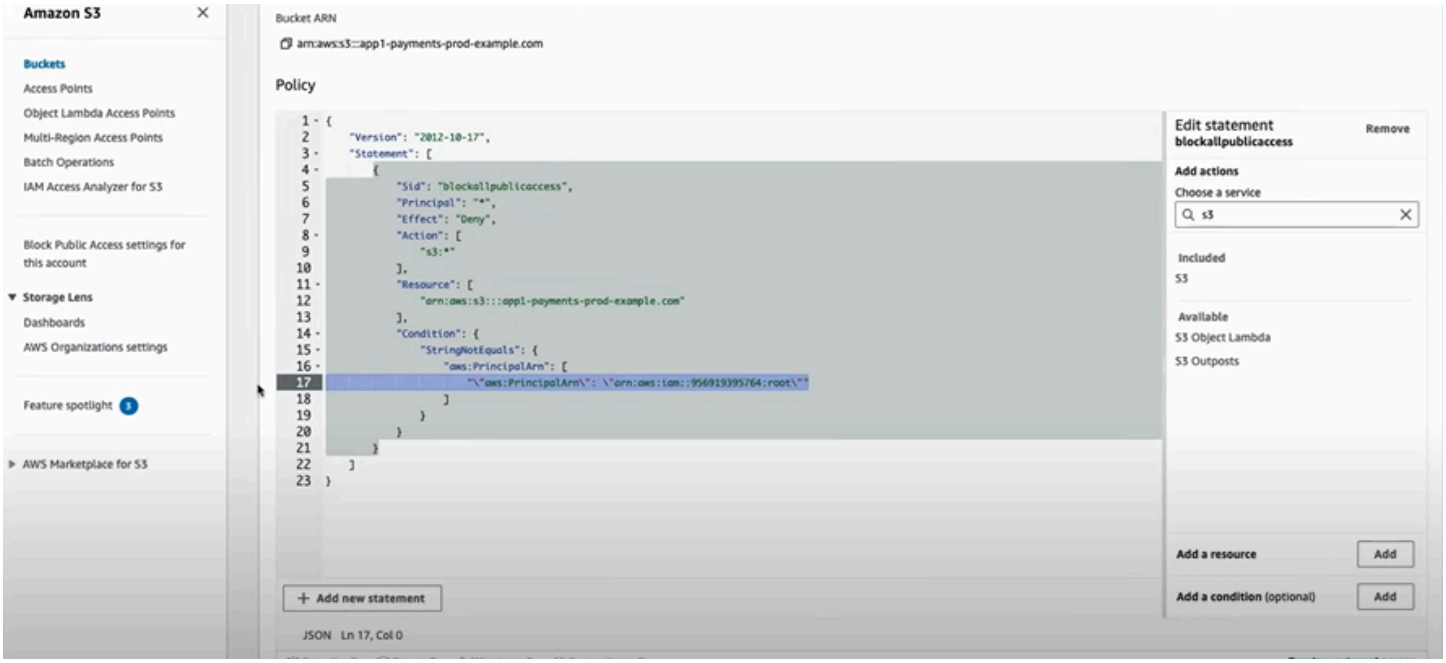
Static website hosting in S3

Amazon S S3 Static Website Hosting is a feature that allows you to host static websites directly from an S3 bucket. A static website serves content (HTML, CSS, JavaScript, images, etc.) that does not change based on user interactions, making it an ideal solution for simple websites, landing pages, and web applications that don't require server-side processing.



1. Make public access enable
2. Attach a policy (above) to make all the users access the static website.

Bucket policy example



it says, principal → againts whom ? → * means everybody

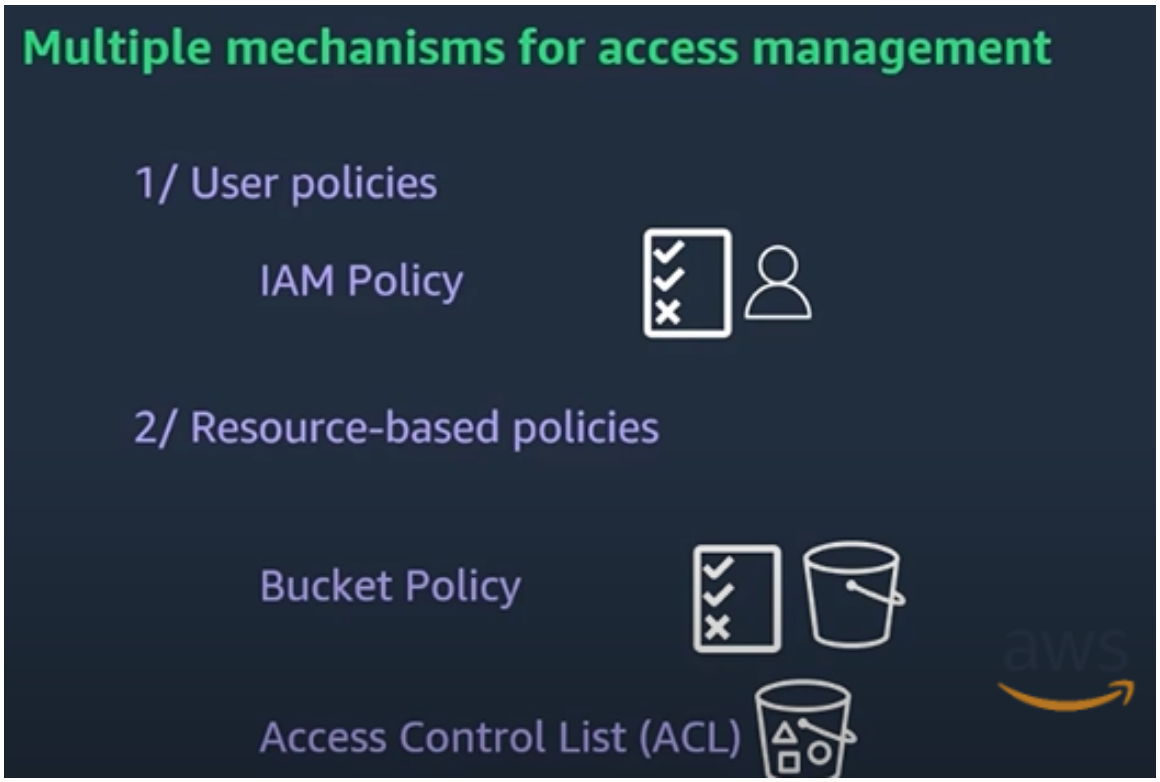
effect → deny access

action → every action related to s3

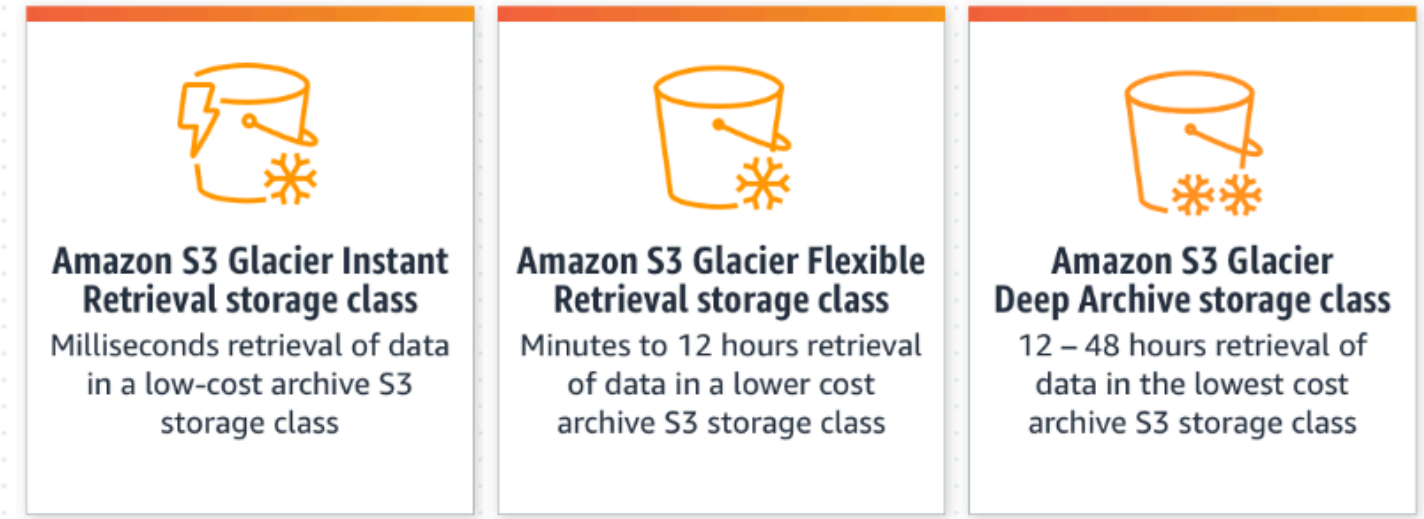
resource → the particular s3 bucket should be specified

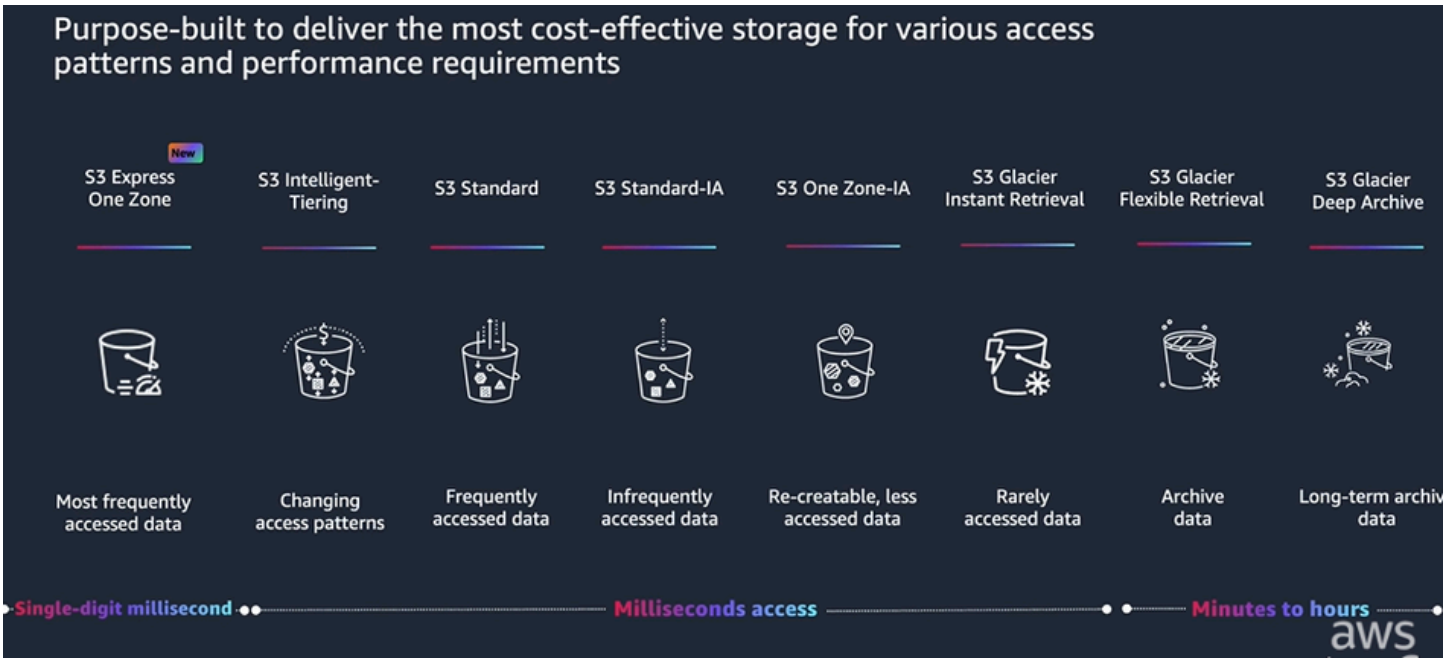
condition → except me deny access for everyone

AWS POLICIES

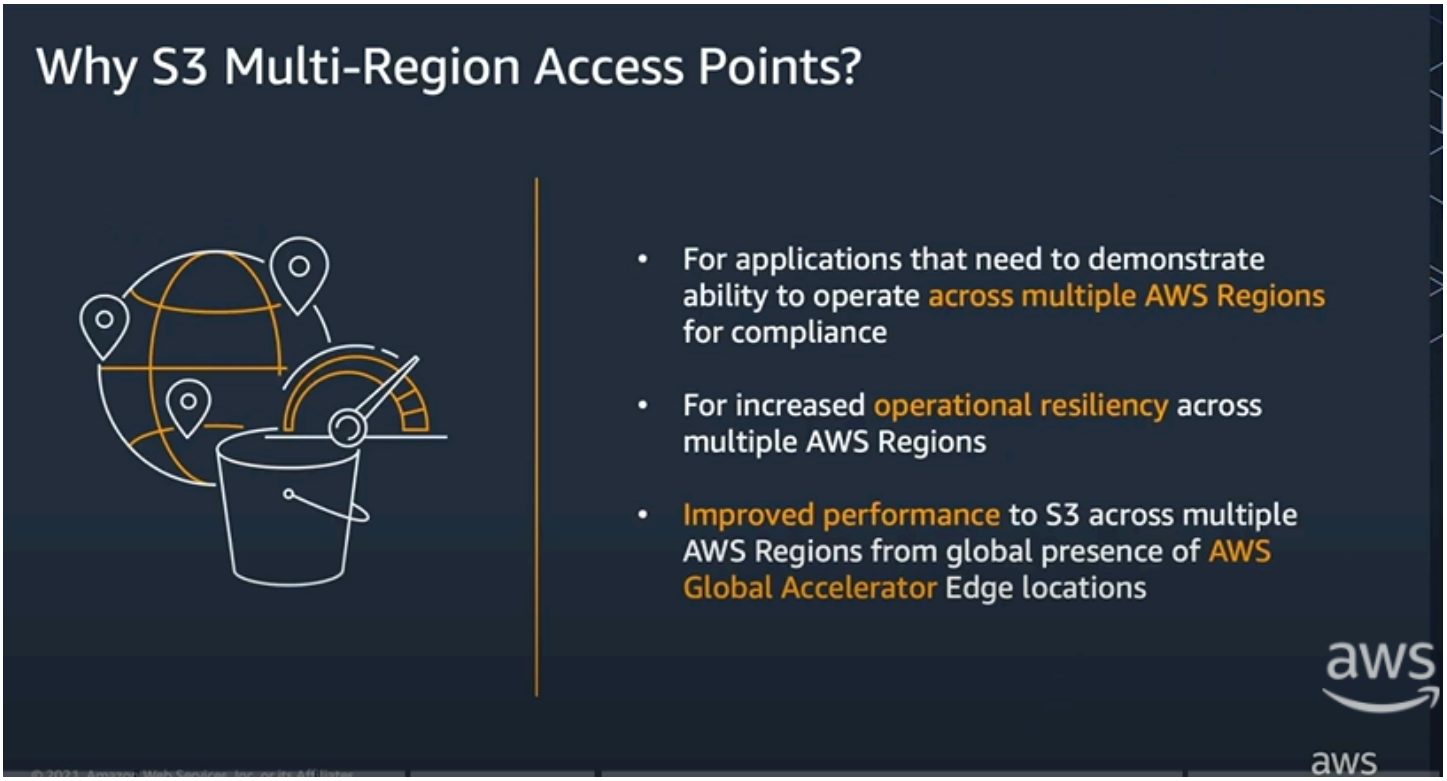

Multiple mechanisms for access management
1/ User policies
IAM Policy
2/ Resource-based policies
Bucket Policy
Access Control List (ACL)
aws

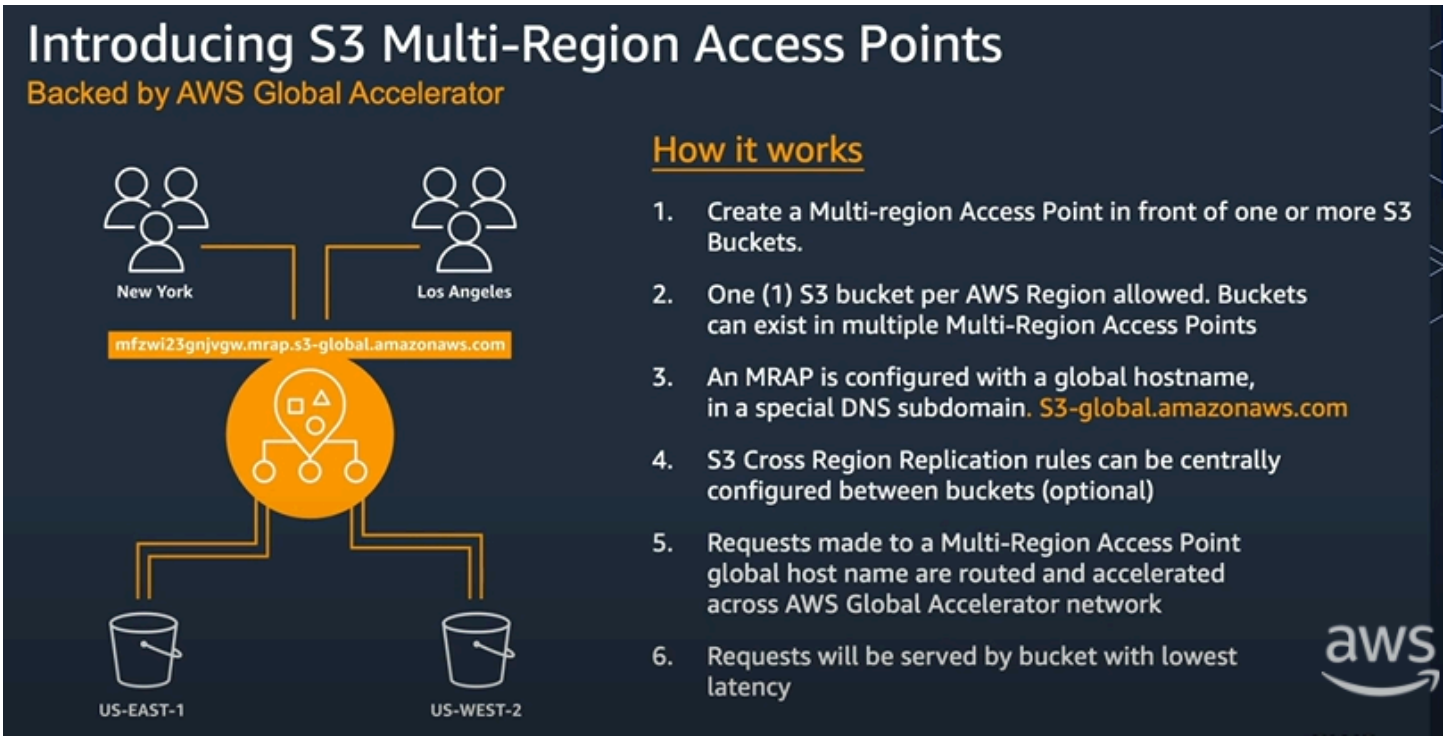
S3 Glacier

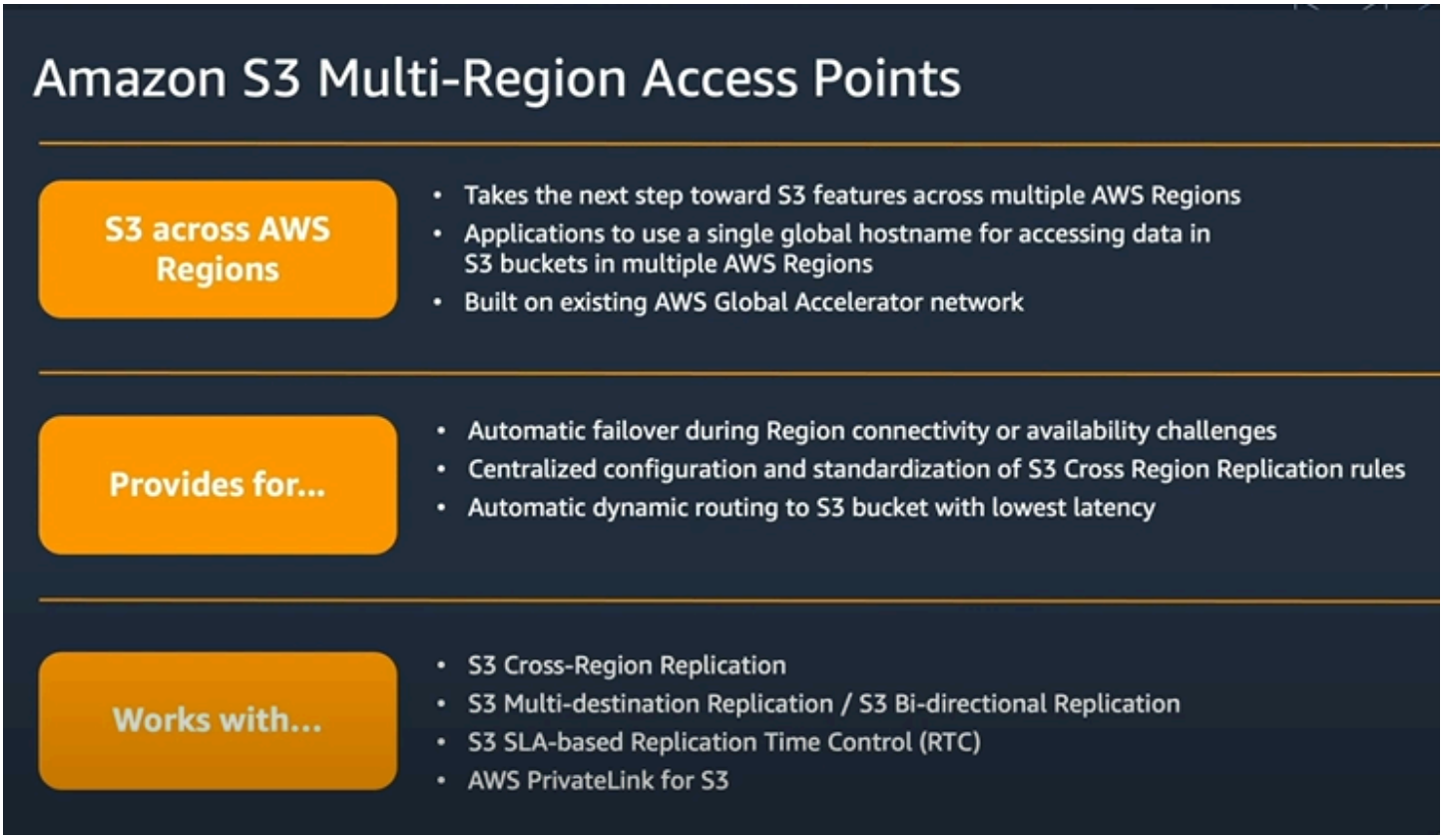

Amazon S3 Glacier Instant Retrieval storage class
Milliseconds retrieval of data in a low-cost archive S3 storage class
Amazon S3 Glacier Flexible Retrieval storage class
Minutes to 12 hours retrieval of data in a lower cost archive S3 storage class
Amazon S3 Glacier Deep Archive storage class
12 – 48 hours retrieval of data in the lowest cost archive S3 storage class



S3 Regions and Bucket placement :







More about AWS Access Points:

When the application grows , it becomes more complex to set and maintain the bucket policies , so to address this problem aws comes up with different access points.

The Problem

- There is an S3 bucket and it is used to store data that is shared among different applications/teams with different levels of access requirement.
- With time, the S3 bucket policy becomes big, gets regularly updated & hence difficult to audit.
- It is one per bucket and there is a limit on its size.
- This single policy is responsible for controlling access of dozens to hundreds of applications/teams to a bucket.

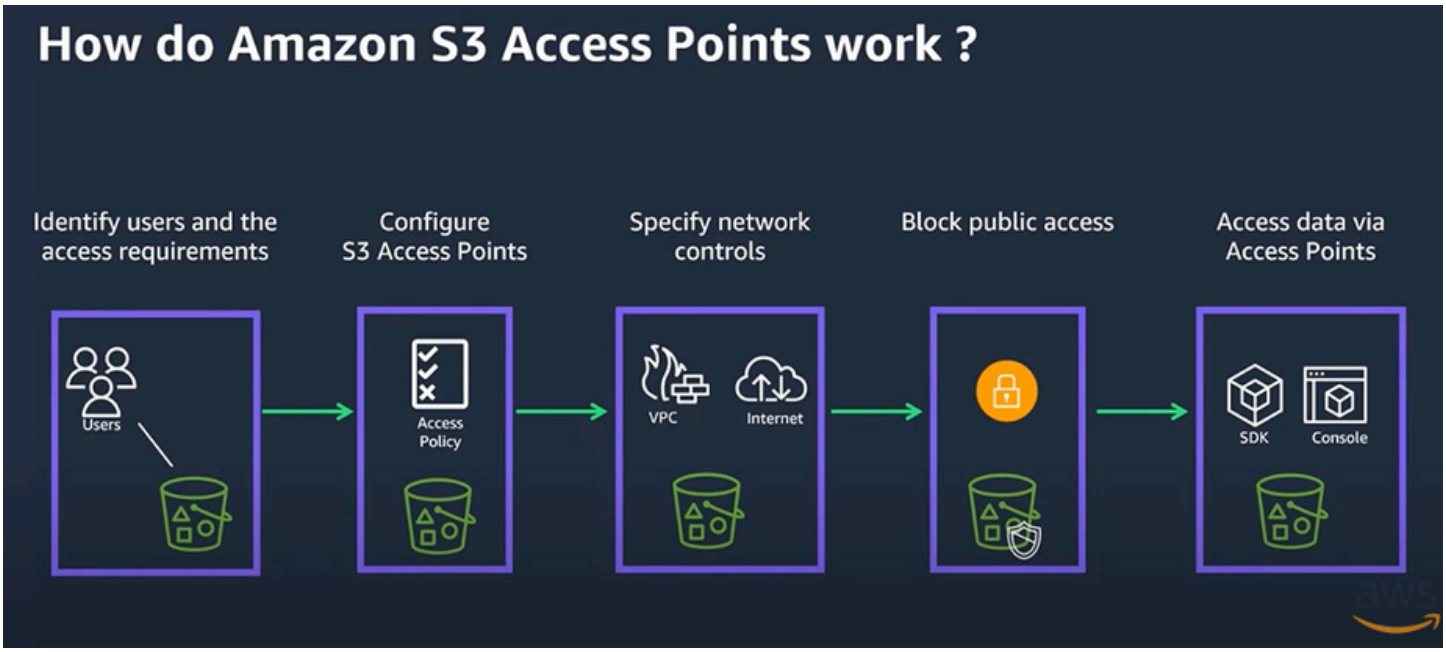
- You can create multiple Access Points for a bucket and the overall management & scaling becomes simpler.

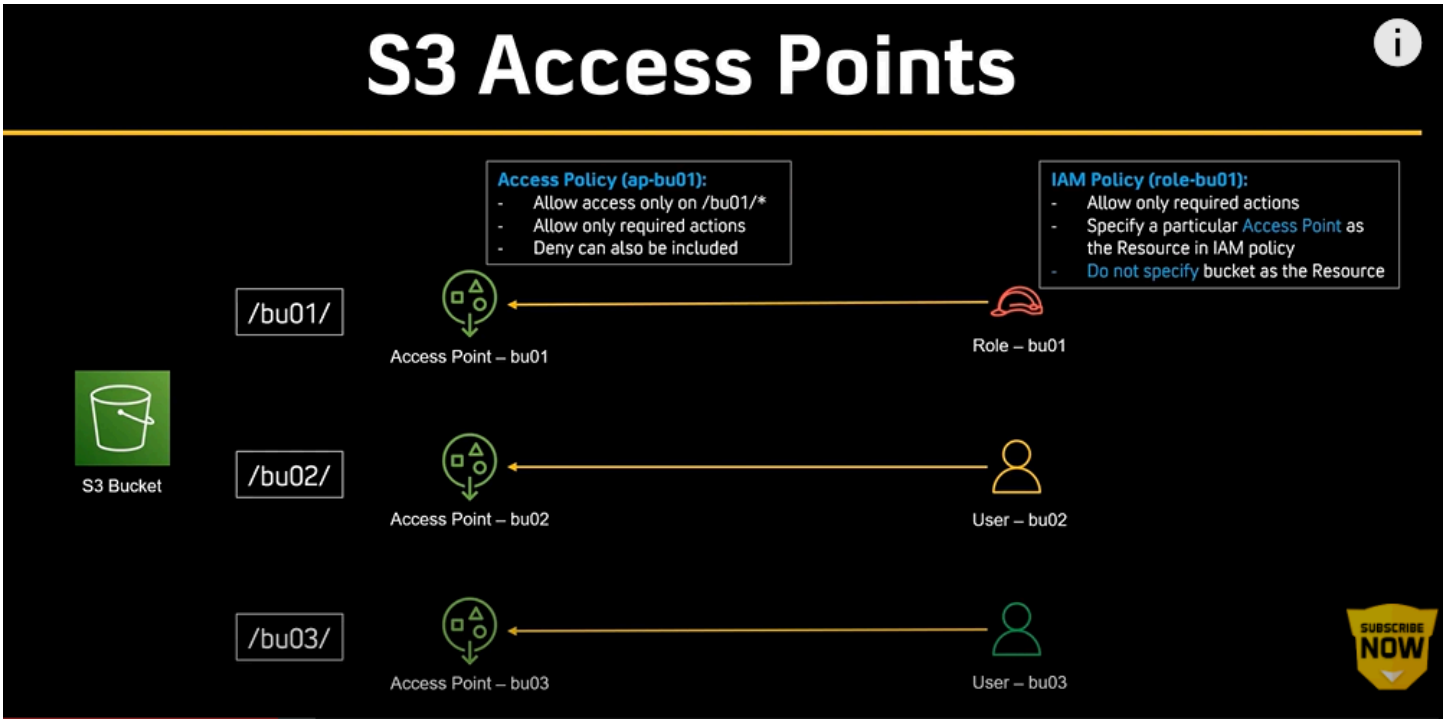
S3 Access Points Introduction

AMAZON S3 ACCESS POINTS MAKES IT SIMPLE TO MANAGE ACCESS AT SCALE FOR APPLICATIONS USING SHARED DATASETS ON S3

- Create multiple access configurations per S3 bucket, each with:
  - Customized path into a bucket
  - Unique hostname
  - Access policy
  - Network controls for requests

No additional cost for access points . !!



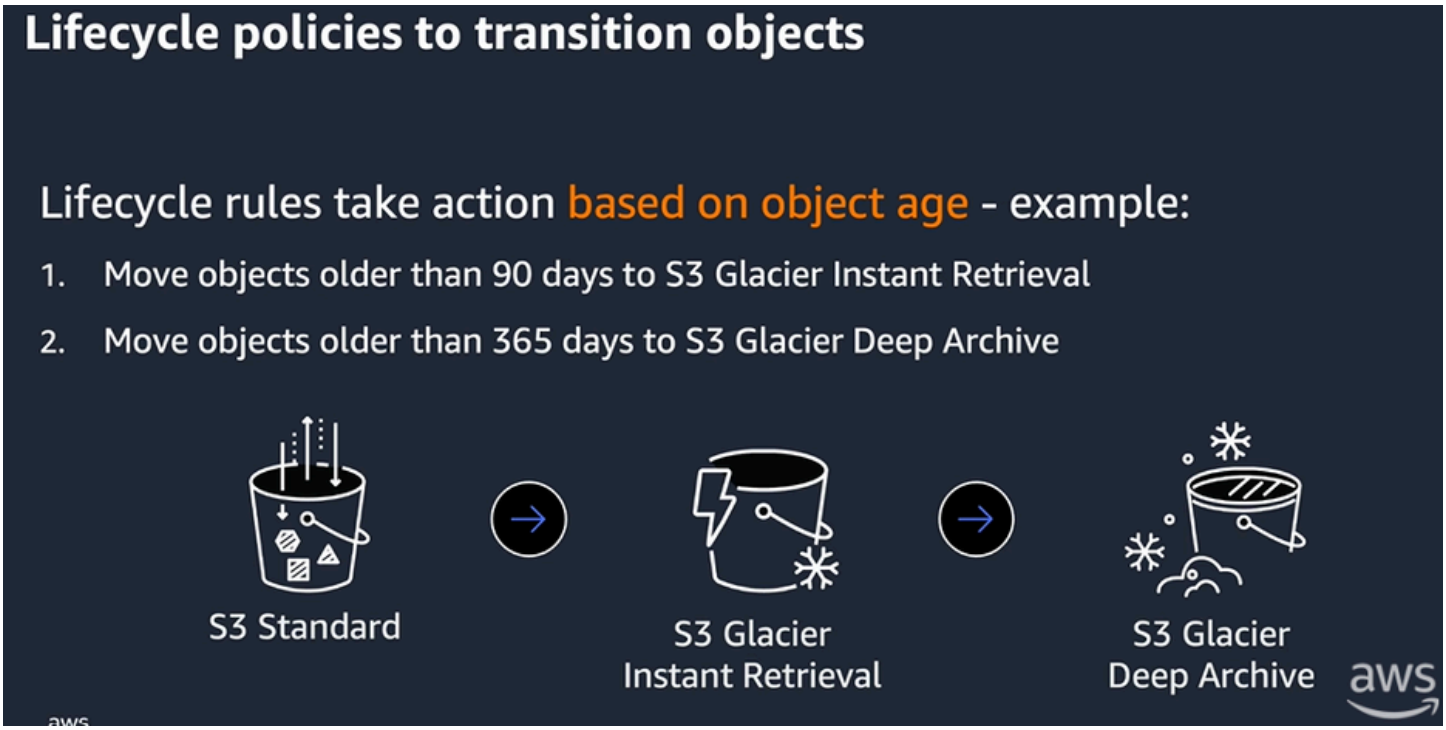


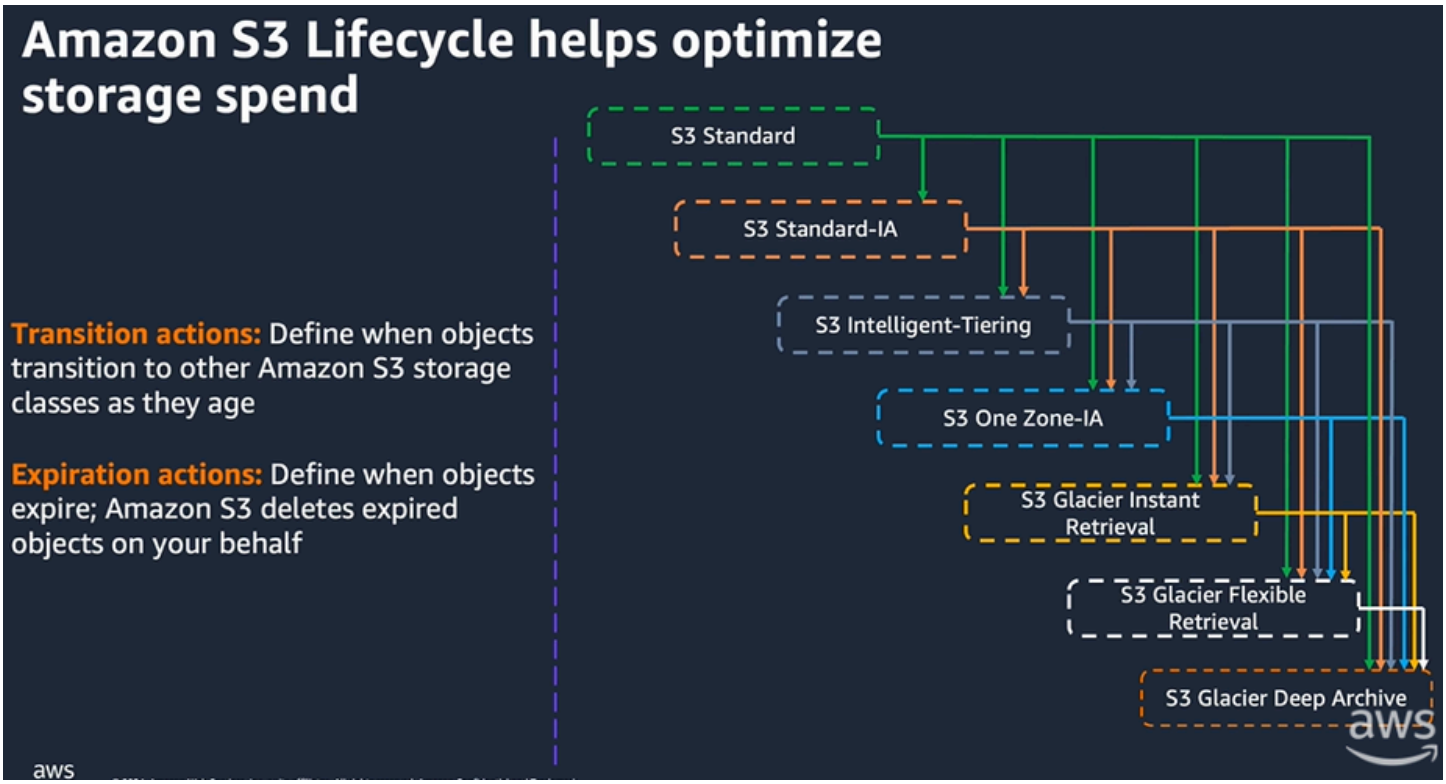
Each access point enforces a customized access point policy that works in conjunction with the bucket policy that is attached to the underlying bucket.

Difference between access point from vpc and internet

Feature	VPC Endpoint (Access Point from VPC)	Internet Access
Connection Type	Private connection via AWS internal network	Public connection via the internet
Traffic Path	Stays within AWS's internal network	Routed through the public internet
Requires Public IP	No	Yes (for EC2 instances or other resources accessing S3)
Security	More secure (no exposure to the public internet)	Less secure (requires encryption and public endpoint protection)
Latency	Lower latency, more predictable	Potentially higher latency, depends on the internet route
Cost	Typically cheaper for large data transfer within AWS	May incur higher data transfer costs due to internet usage
Access Control	Fine-grained access using VPC Endpoint Policies and Access Points	Bucket policies and IAM roles can restrict access
Use Case	Best for accessing S3 privately from within VPC environments	Ideal for access outside AWS (e.g., from users or external services)
Availability	Available within the specific VPC and subnets	Accessible globally via the public internet
Data Encryption	Optional (data remains within AWS network)	Strongly recommended (due to exposure on public internet)
Requires Internet Gateway/NAT	No	Yes (for EC2 instances in private subnets)
S3 Endpoints	Uses a private S3 endpoint like `com.amazonaws.vpce`	Uses the standard S3 public endpoint like `s3.amazonaws.com`

AWS S3 Lifecycle policies





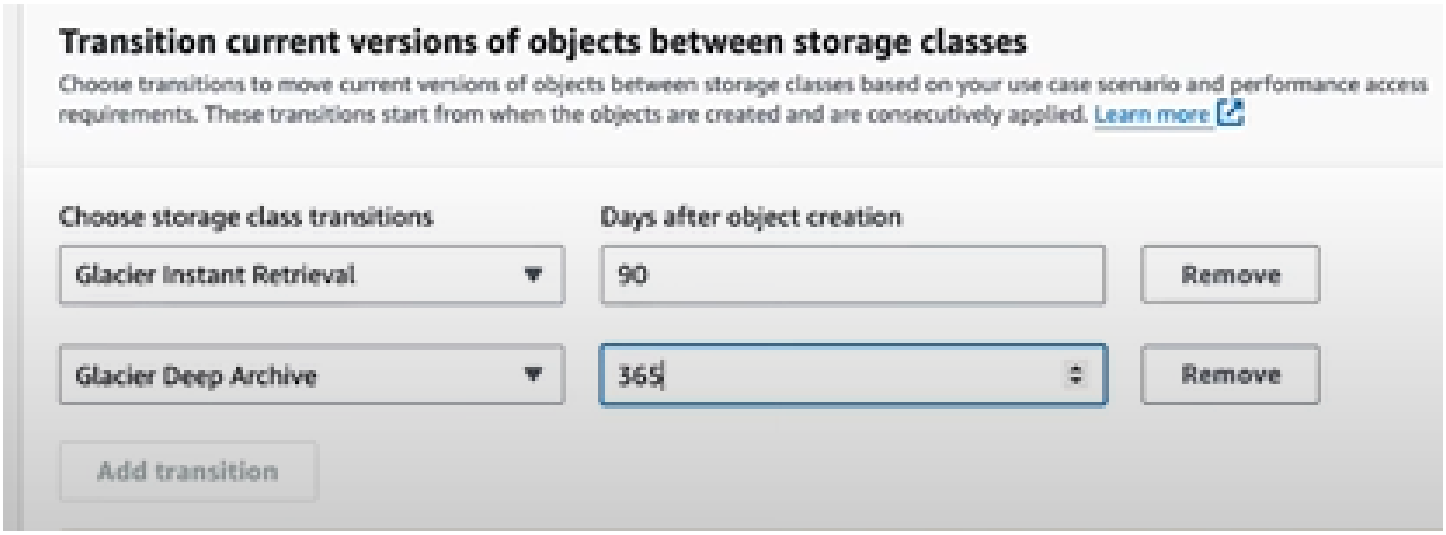
It follows waterfall method (i.e cannot come back after transition)

How to enable lifecycle to a bucket ?

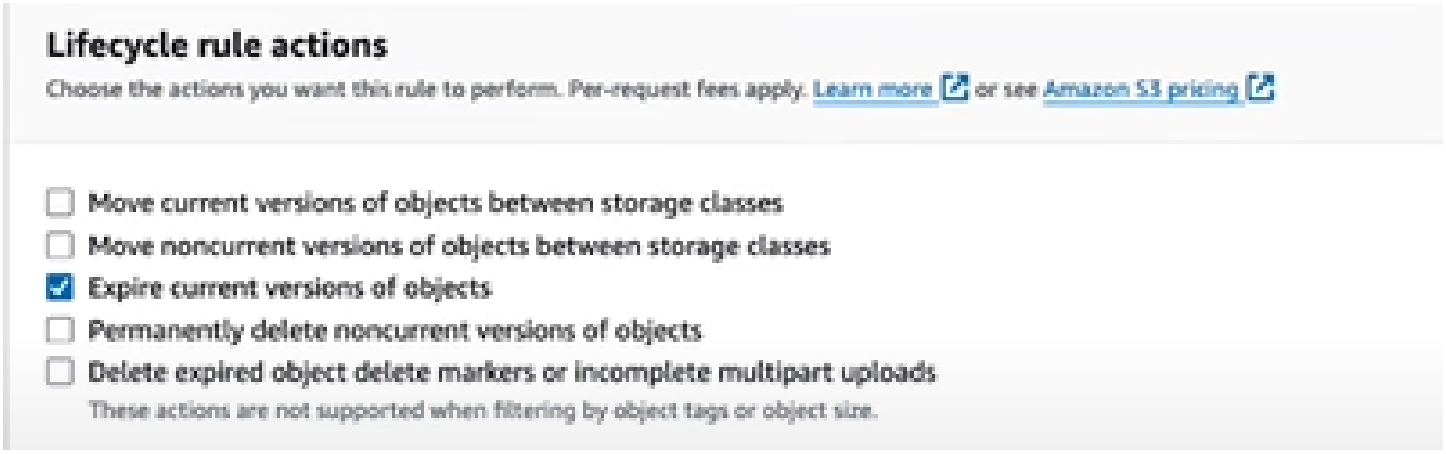
select a bucket → go to management → create life cycle rule

we can apply the rule either to all the objects in a bucket or limit to some objects alone.

we can also mention, like the life cycle policy should apply to objects only of this size (i.e.based on the size)

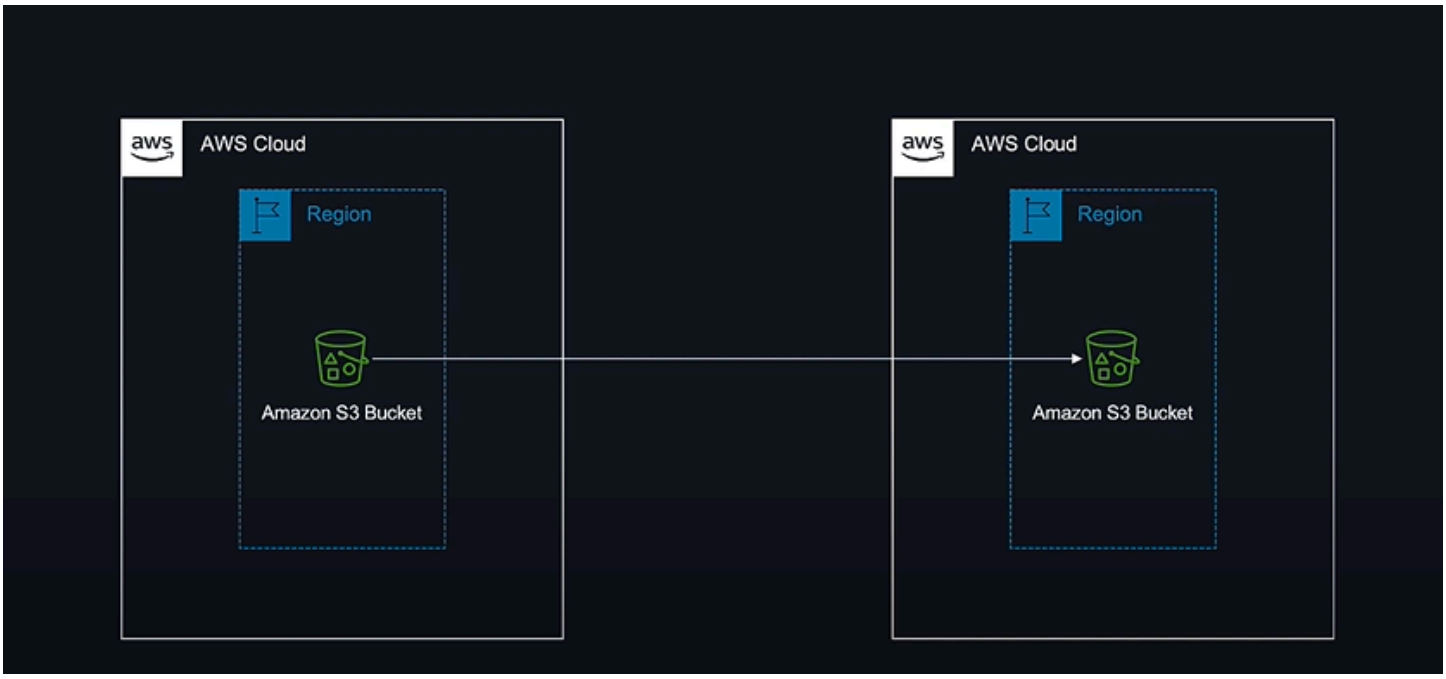


lifecycle rule actions provided by aws ?



S3 Cross Origin Replication :

It is a feature that replicates s3 across different regions.



Source Bucket and Destination Bucket:

Source Bucket: This is the bucket from which objects will be replicated. It's located in one AWS region.

Destination Bucket: This is the bucket where the replicated objects will be stored. It's located in a different AWS region.

You can set the destination bucket to any AWS region other than the source bucket's region.

Practical Guide:

select source bucket → management → replication rules

Note : Bucket versioning is a must to do replication. (Just enable versioning of the bucket)

We can limit replication to specific objects in a bucket or select all objects in a bucket to replicate.

if needed we can specify which storage class the replicated object should be stores (ex: s3 standard , instant glacier ....)

crr only applies to replicate new objects in the object , in order to replicate existing objects we should use batch operations.

AWS S3 Encryption ?

AWS makes sure that data should remain secure in transit and at rest. It has both client side encryption and server side encryption.