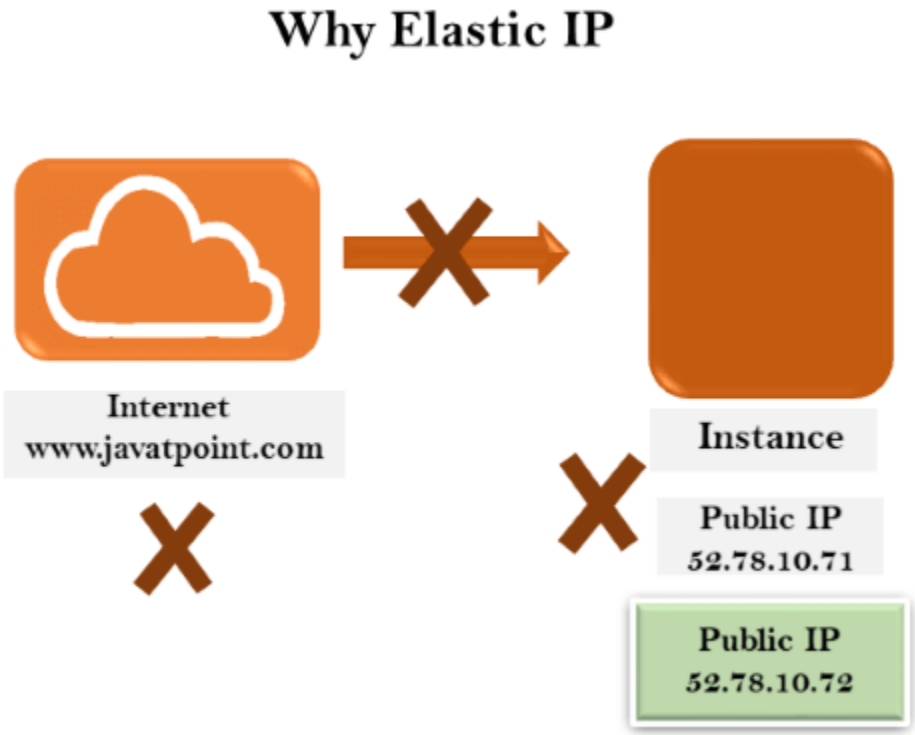
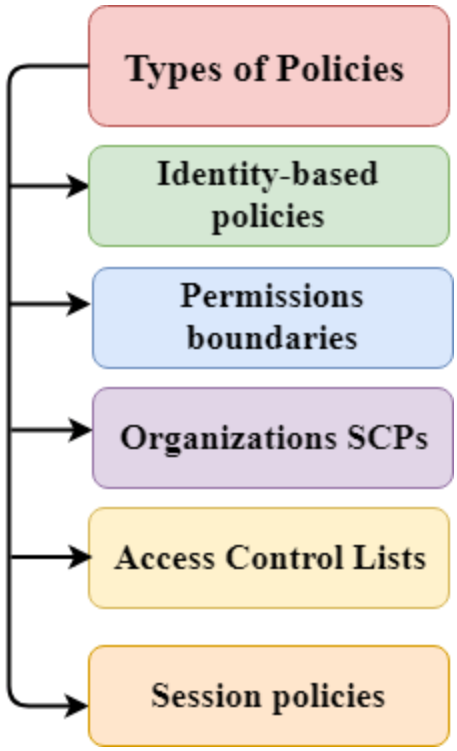
AWS Arch Understanding

understand the concept of EIP



AWS supports six types of policies:

- Identity-based policies
- Resource-based policies
- Permissions boundaries
- Organizations SCPs
- Access Control Lists
- Session policies

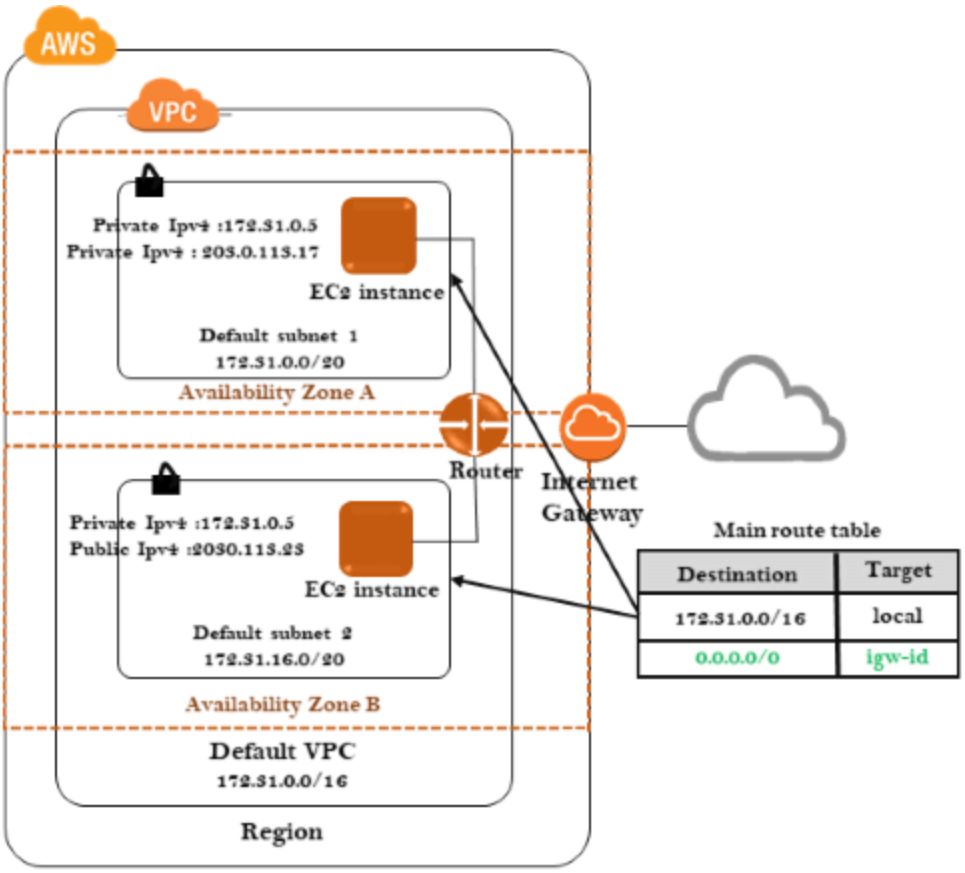


There are two types of access:

- **Console Access**
  If the user wants to use the Console Access, a user needs to create a password to login in an AWS account.
- **Programmatic access**
  If you use the Programmatic access, an IAM user need to make an API calls. An API call can be made by using the AWS CLI. To use the AWS CLI, you need to create an access key ID and secret access key.

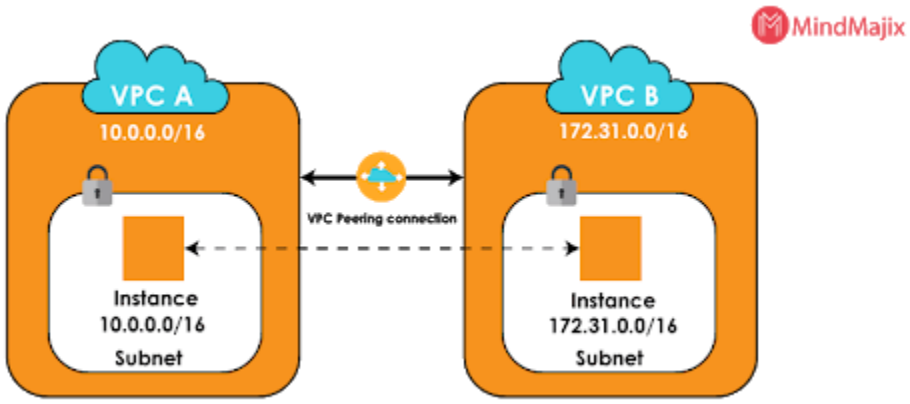
subnet

When large section of IP address is divided into smaller units is known as subnet.



Amazon VPC

Amazon VPC is known as Amazon Virtual Private Cloud (VPC), allowing you to control your virtual private cloud. Using this service, you can design your VPC right from resource placement and connectivity to security. And you can add Amazon EC2 instances and Amazon Relational Database Service (RDS) instances according to your needs. Also, you can define the communication between other VPCs, regions, and availability zones in the cloud.



AWS Elastic Beanstalk

1. In a way, it is faster and simpler to deploy applications
2. The auto-scaling facility of Elastic Beanstalk supports to scale applications up and down based on the demands.

3. This AWS service manages application platforms by updating with the latest patches and updates.

4. When they use this service, developers could achieve enough freedom to choose the type of EC2 instance, processors, etc.

What is EC2

Amazon EC2 or Amazon Elastic Compute Cloud is a cloud service that enables secure and resizable compute capacity. It makes web-scale cloud computing simpler for developers

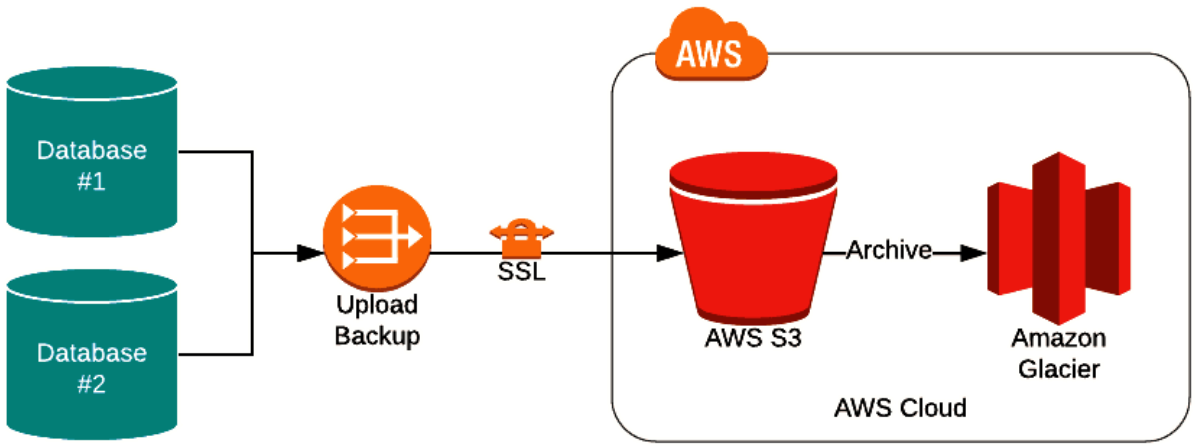
Snowball

Snowball is a small petabyte-scale data that enables transferring huge quantities of data inside and outside the AWS Cloud.

Cloud Watch

AWS CloudWatch enables the monitoring of AWS environments like RDS Instances, EC2, CPU utilization

S3



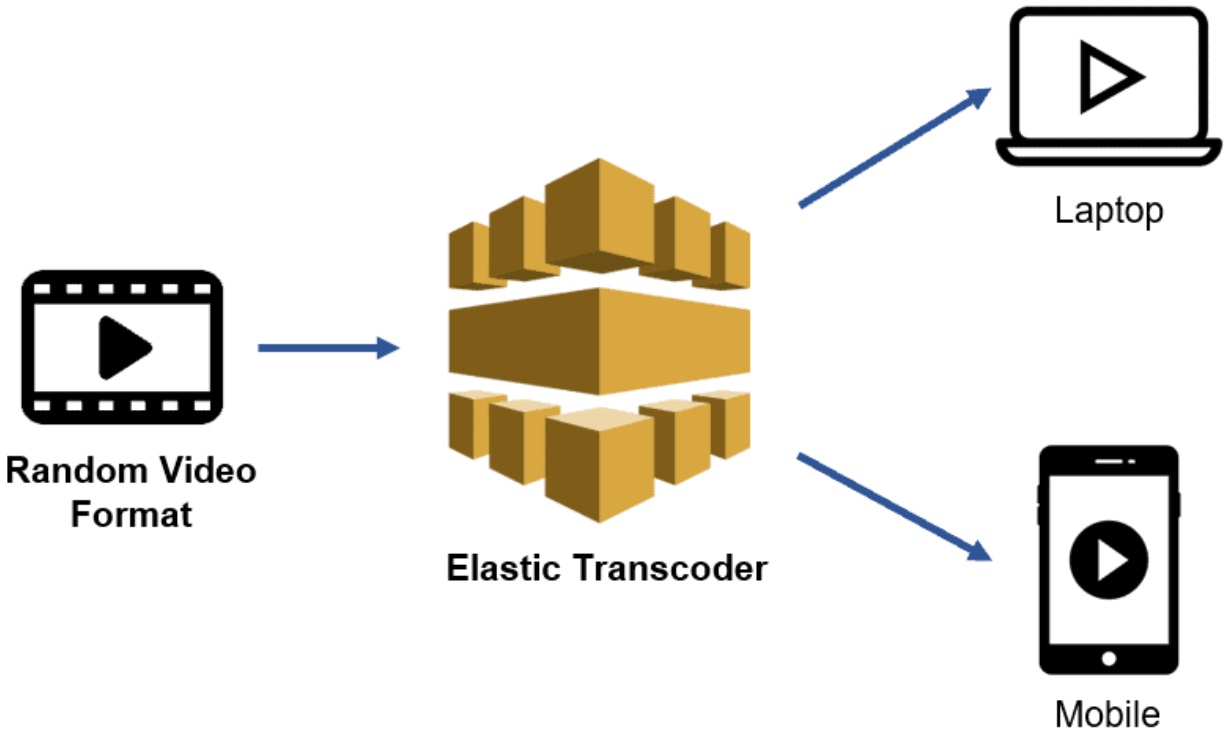
Amazon S3 or Simple Storage Service is a storage service that makes web-scale computing easier. The simple interface is used to store and retrieve data at any time from anywhere over the internet.

Storage Classes available in Amazon S3

Different Storage Classes available in Amazon S3 are:

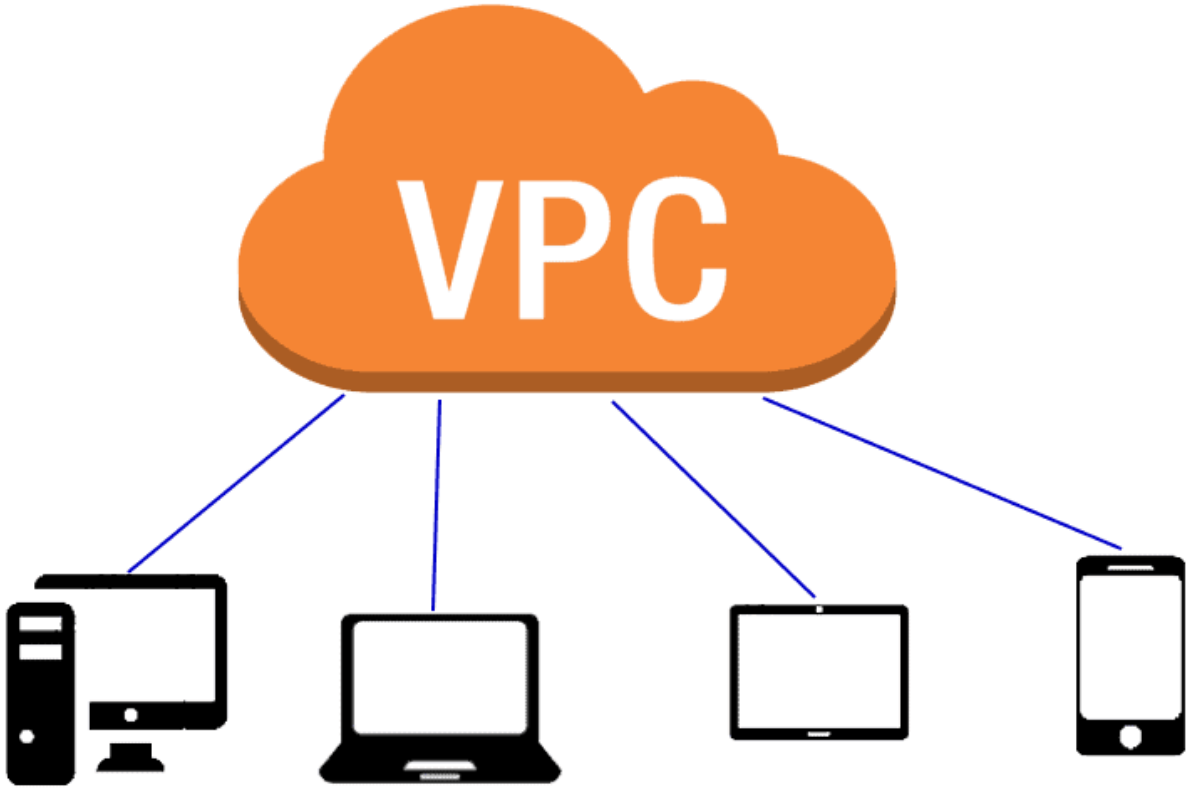
- Amazon S3 standard
- Amazon S3 standard – infrequent Access
- Amazon S3 Reduced Redundancy
- Storage Amazon Glacier

Elastic Transcoder



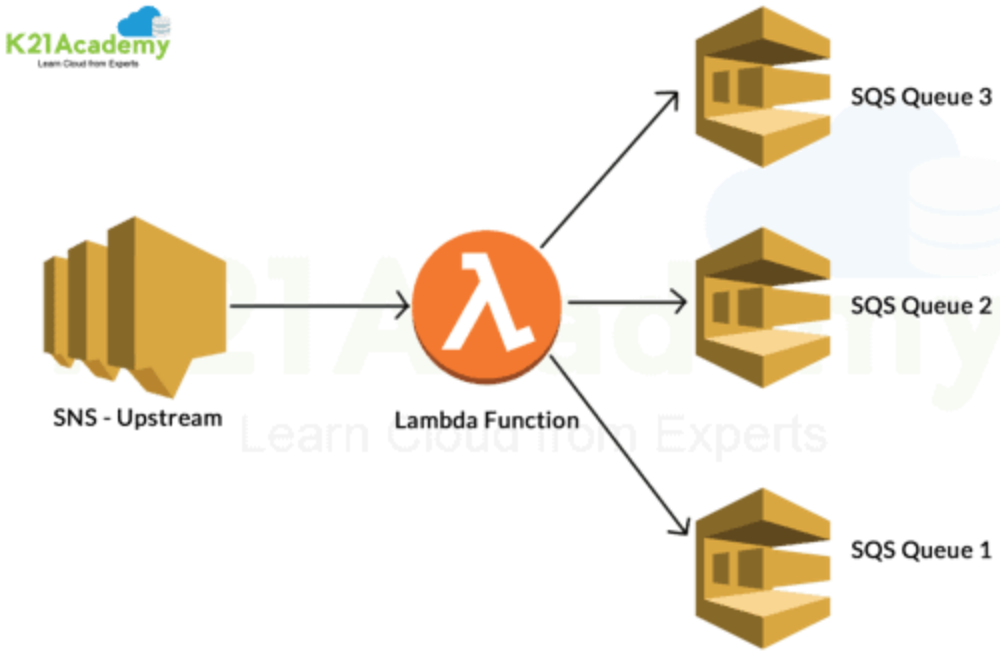
Elastic Transcoder is an Amazon media transcoding service tool used to convert media files like videos in terms of format and resolution for different resolution devices like phones, laptops, etc.

VPC



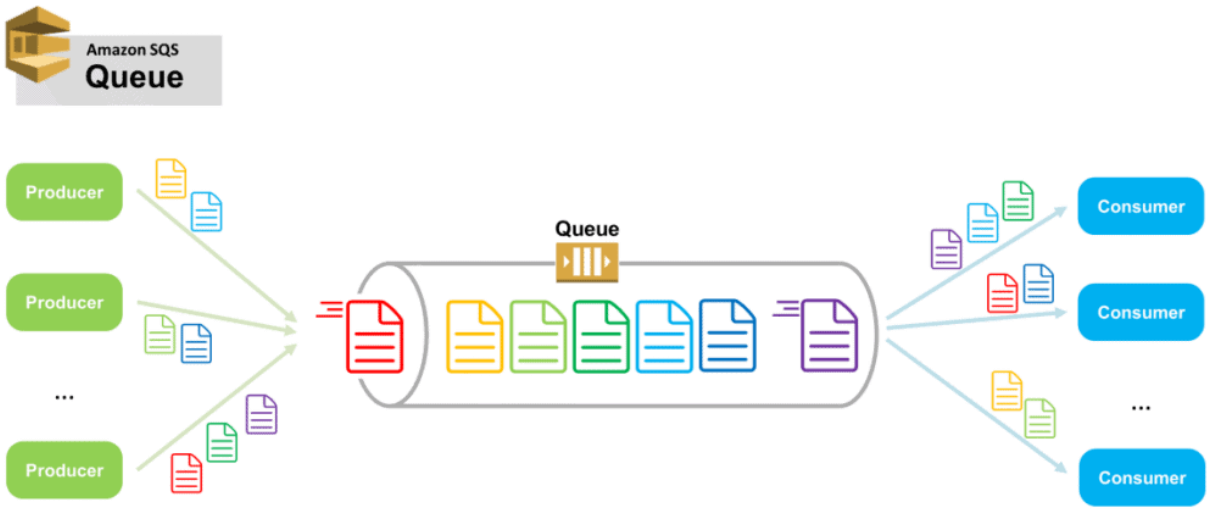
Amazon VPC or Virtual Private Cloud is an Amazon service that enables AWS resources to be in a logically isolated virtual network.

AWS Lambda



AWS Lambda is an Amazon serverless compute service that enables code to run without managing servers in the AWS cloud.

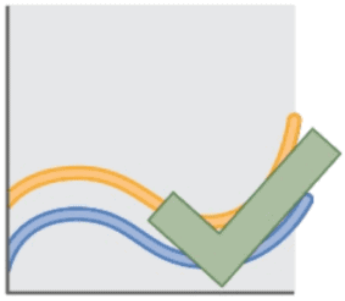
SQS



Amazon SQS or Simple Queue Service is a fully managed Amazon message queuing service that makes decoupling and scaling microservices and distributed systems possible.

Auto-Scaling

Elastic:
Automatically adapt capacity to demand



Reliable:
Counteract failures of instances or AZs

Customizable:
With bootstrapping & lifecycle hooks

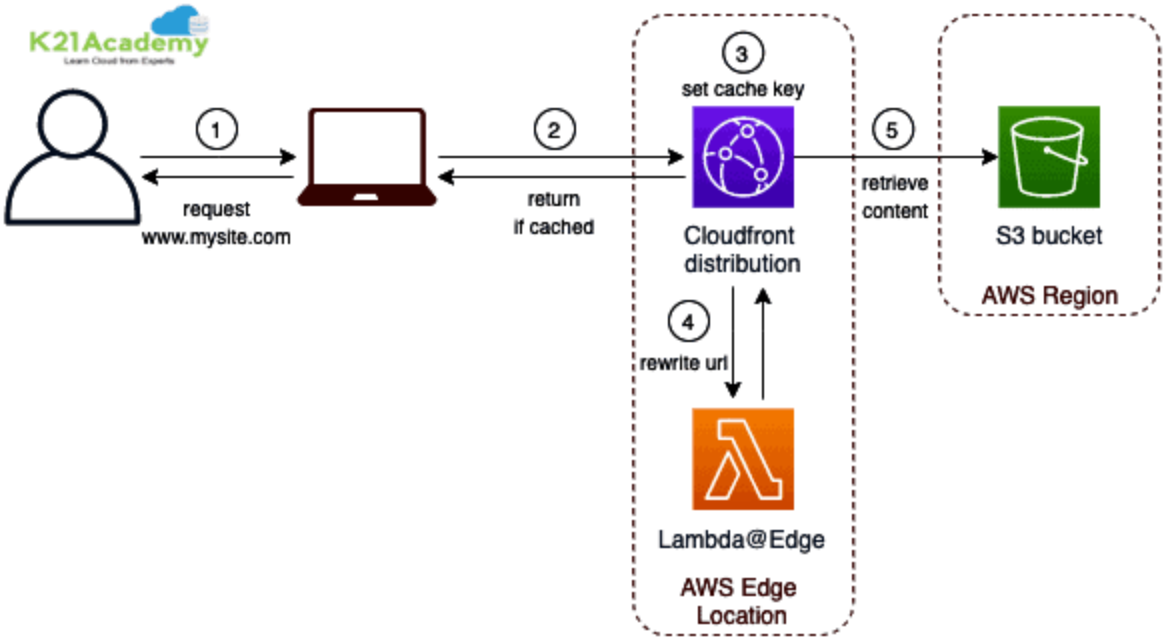
The advantages of auto-scaling are:

- Better availability
- Better fault tolerance
- Better cost management

Amazon EC2 and Amazon S3

Amazon EC2	Amazon S3
• Amazon EC2 is an Amazon web service that enables the hosting of applications. • It can run on both Windows and Linux and handle applications like PHP and Python.	• Amazon Simple Storage Service is a data storage service where huge amounts of any data are stored. • It works on a REST interface and enables the storing and retrieving of data at any time over the web.

CloudFront

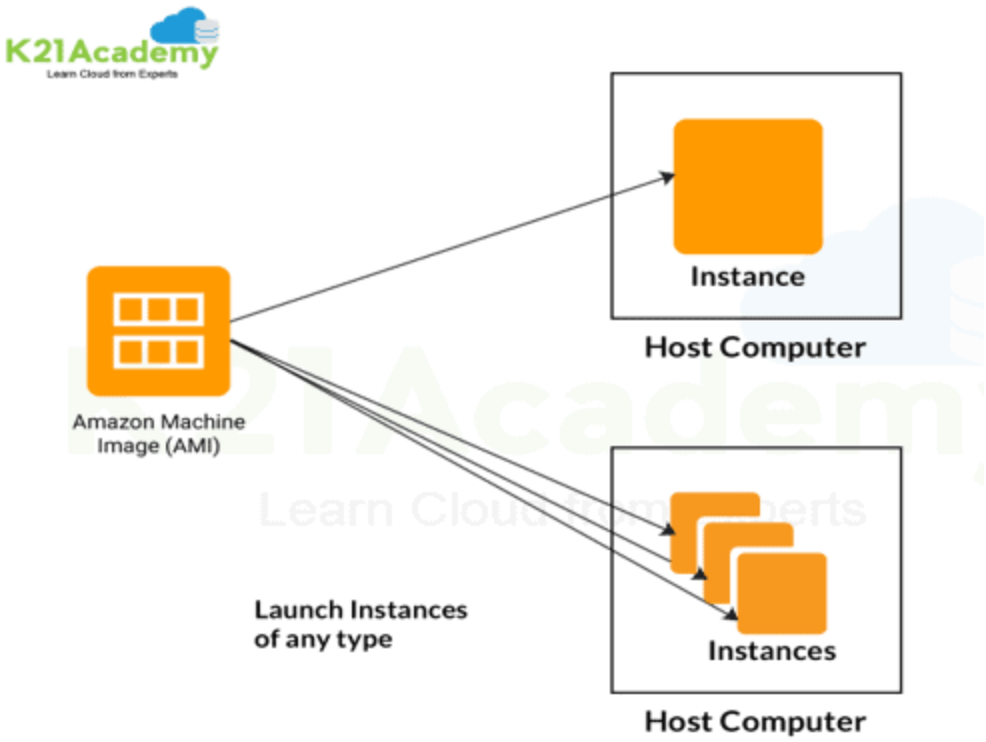


Geo-targeting in CloudFront enables the detection of the user's origin country and country code. It helps businesses to show personalized content according to their geographic video.

Cloud Services

- Software as a Service (SaaS)
- Data as a Service (DaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

AMI include



AMI include:

- A template for the root volume for a specific type of instance.
- Launch permissions for AWS account to avail AMI to launch instances.
- A block device mapping to ensure correct volumes to the launched instance.

Name the different types of Instances.

Different types of instances are:

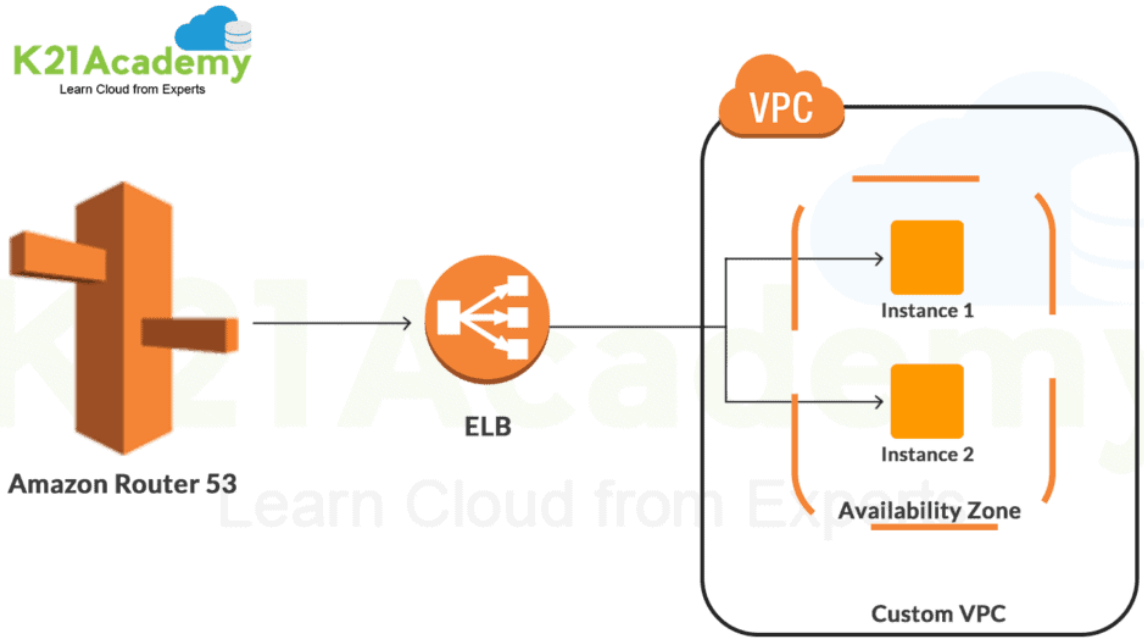
- Compute Optimized
- Memory-Optimized
- Storage Optimized
- Accelerated Computing
- General Purpose

features of AWS IAM

- Enhanced security
- Granular control
- Temporary credentials
- Analyze access
- Flexible security credential management

- Leverage external identity systems

Amazon Route 53

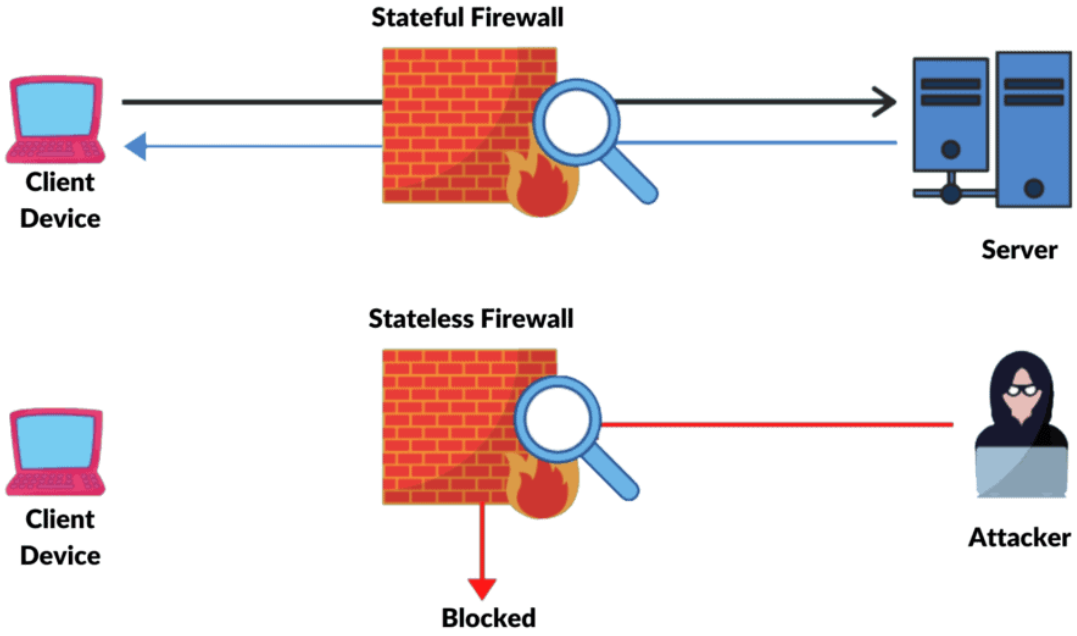


Amazon Route 53 is an Amazon web service for scalable and highly available DNS (Domain Name System). The number 53 in the name refers to TCP or UDP port 53, where DNS server requests are addressed.

Amazon Route 53 uses three important things to provide high availability and low latency.

- Globally Distributed
- Server Dependency
- Optimal Locations

Stateful and Stateless Firewall

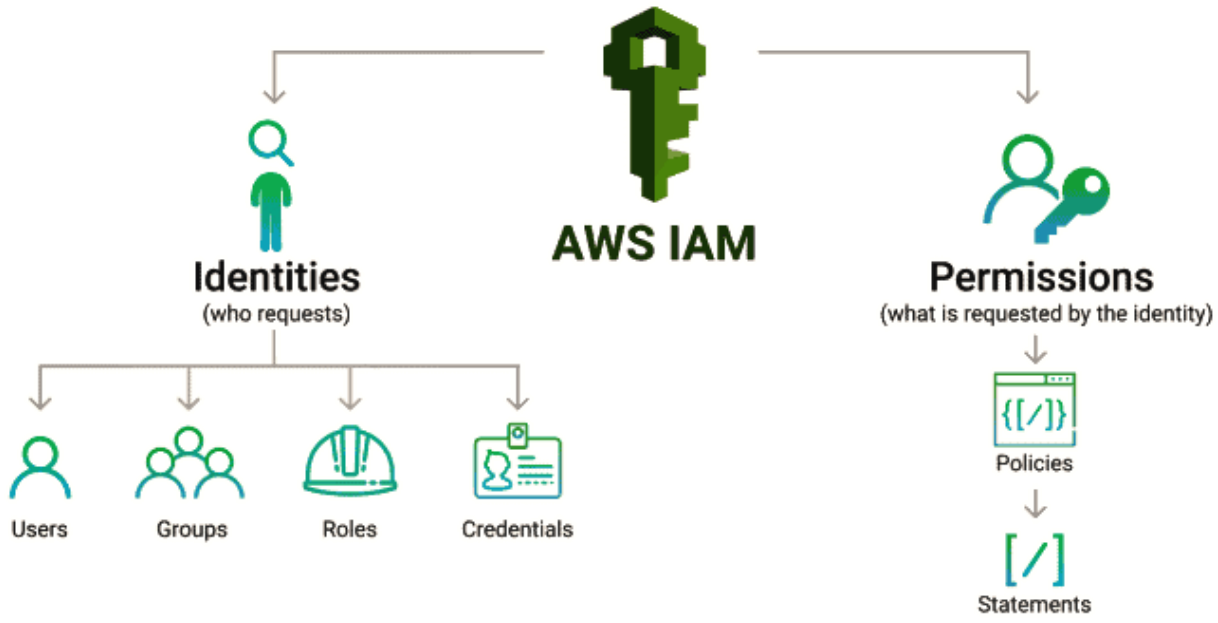


- Stateful Firewall maintains the state of defined rules. Based on the defined inbound rules, it lets the outbound rules flow. Stateful firewalls can monitor and detect the states of all traffic on a network in order to track and defend against traffic patterns and flows.
- A stateless Firewall needs explicitly defined rules for inbound and outbound traffic. Stateless firewalls are intended to protect networks using static information such as source and destination addresses.

Connection Draining

Connection Draining enables the servers to serve their current requests before they are updated or removed. Connection draining helps re-route the traffic from the Instances and is in a queue to be updated.

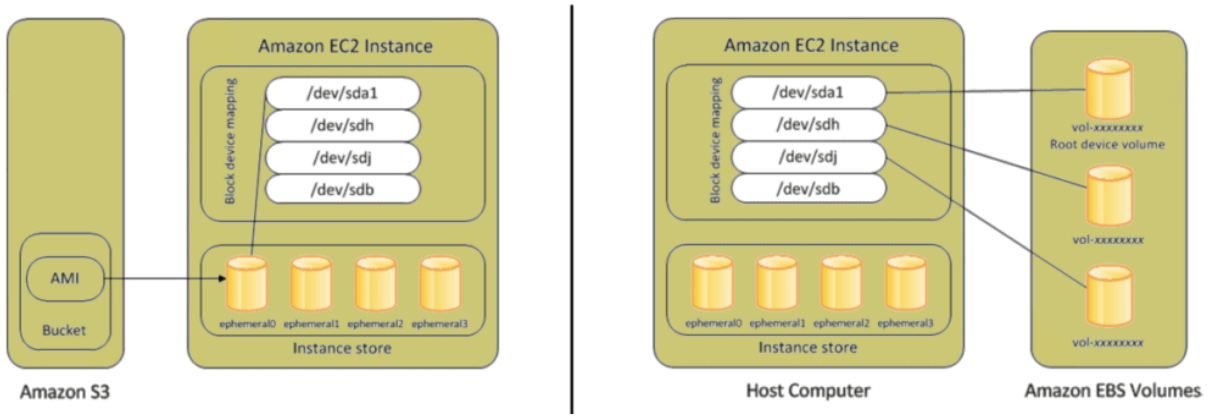
IAM



Power User Access in AWS

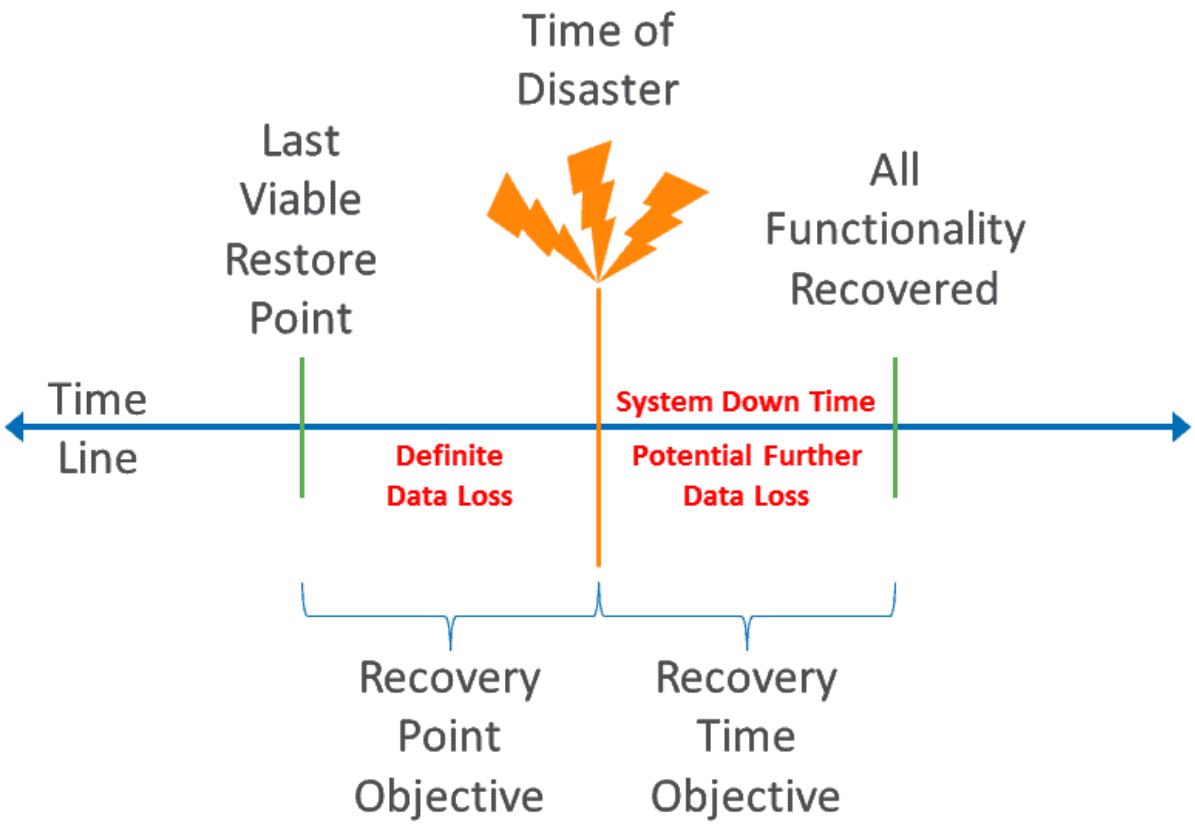
Power User Access is the Administrator Access to create, delete, and modify resources. But, the Administrator user cannot control users and permissions, i.e., they cannot permit others.

Instance Store Volume and an EBS Volume



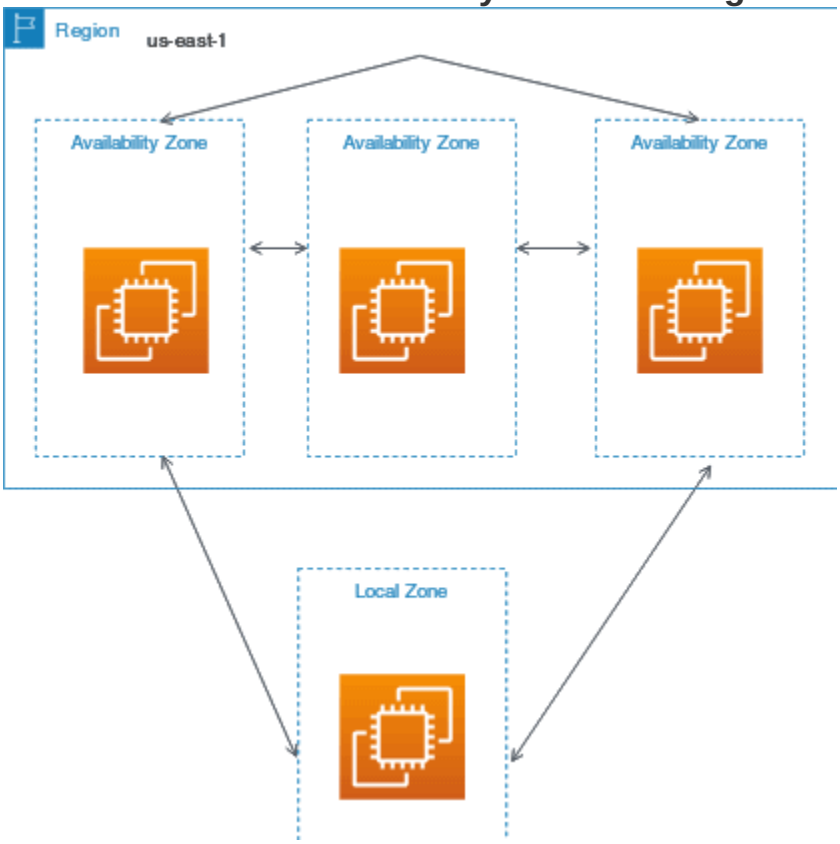
- Instance Store Volume is temporary storage to store temporary data by an instance to a function.
- EBS Volume is a persistent storage disk that is available even when the instances are turned off.

Recovery Time Objective and Recovery Point Objective



- Recovery Time Objective is the maximum delay that is acceptable between the interruption and restoration of service.
- Recovery Point Objective is the maximum delay that is acceptable since the last data restore point.

Relation between Availability Zone and Region



- AWS regions are individual geographic areas like Asia South (Mumbai) and US-west 1 (North California).
- Availability Zones are isolated locations within the regions that can replicate whenever needed.

services to use for collecting and processing e-commerce data

amazon REDSHIFT

amazon DynamoDB

different types of Virtualization in AWS

Different types of virtualization in AWS are:

- Hardware Virtual Machine

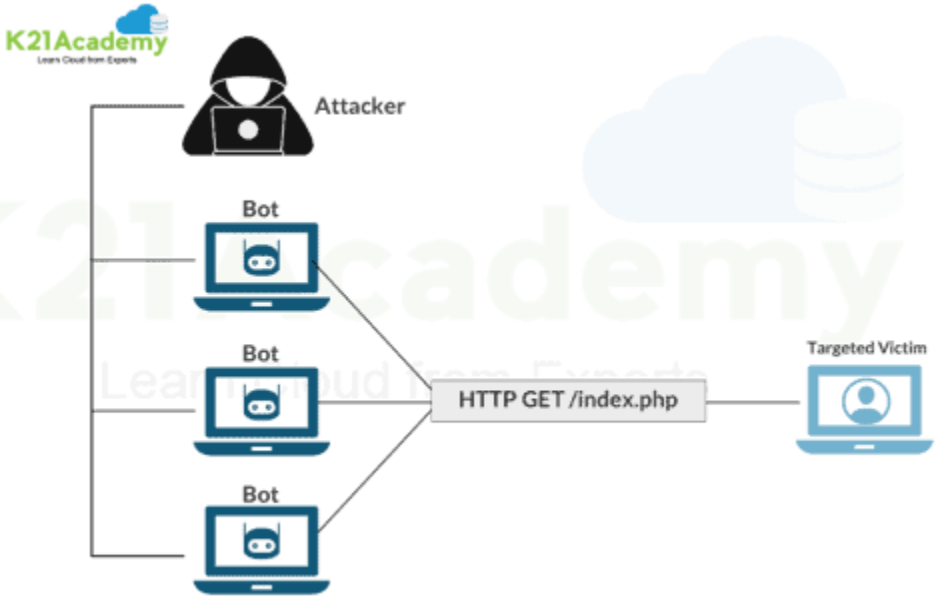
- Paravirtualization
- Paravirtualization on HVM

monitor Amazon VPC

Amazon VPC can be monitored in the following ways:

- CloudWatch and CloudWatch logs
- VPC Flow Logs

DDoS attacks, and What Services can minimize them

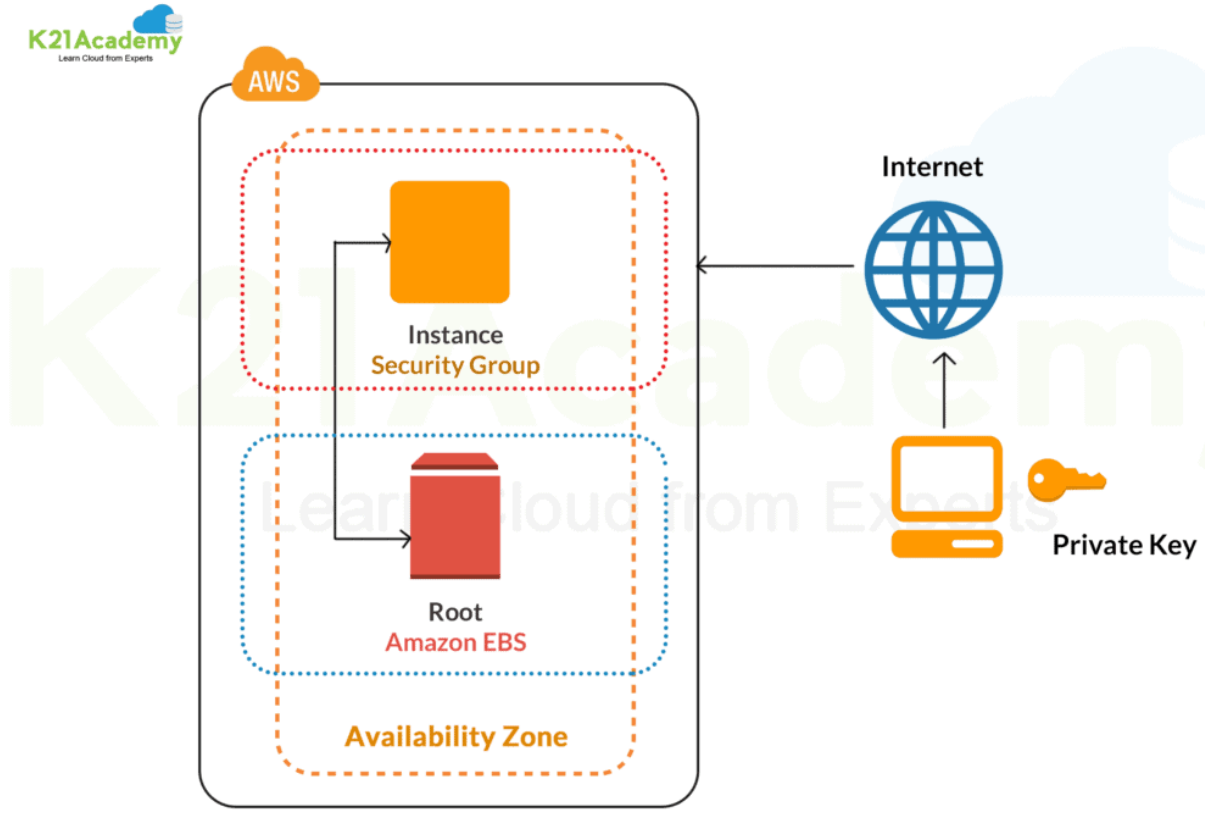


AWS Services that are not Region Specific

ome of the non-region-specific AWS services are:

- IAM
- Route 53
- Web Application Firewall
- CloudFront

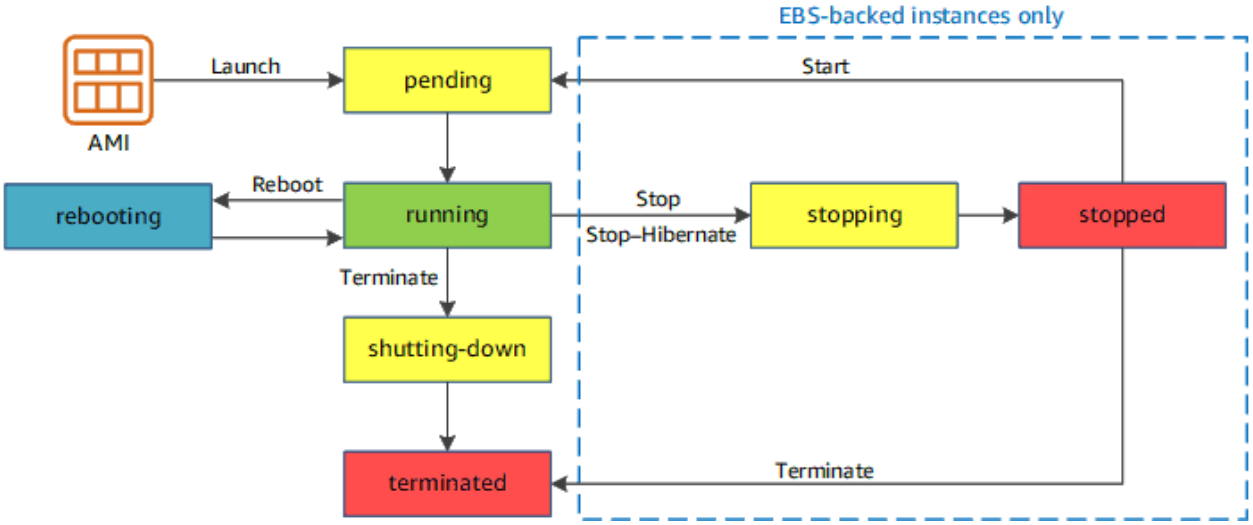
Security Best Practices for Amazon EC2



Security best practices for Amazon EC2 are:

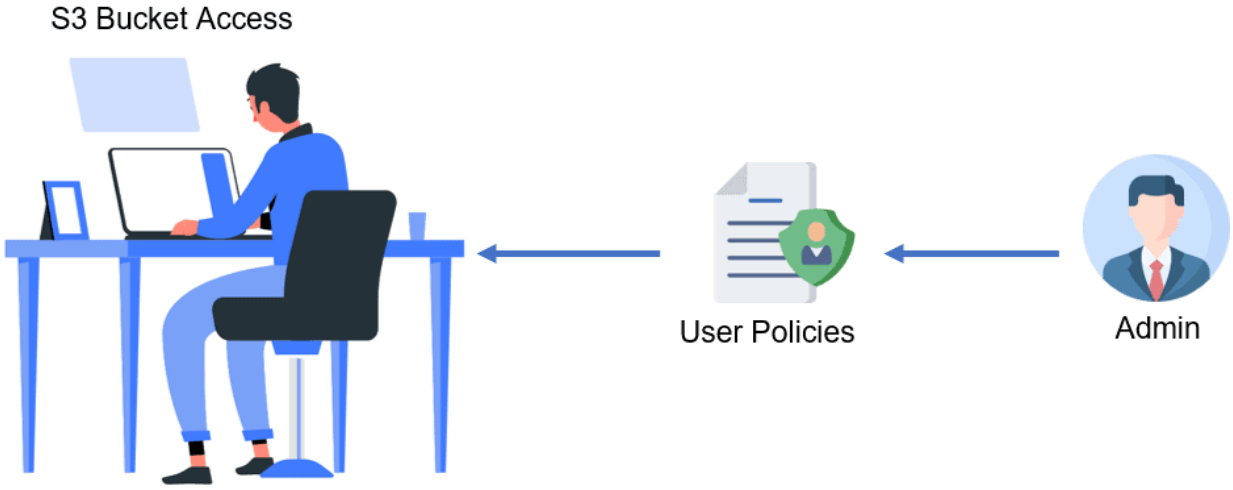
- Only allowing the trusted hosts or networks to access ports on an instance.
- Using Identity and Access Management (Identity and Access Management) to control access to AWS resources.
- Only enabling those permissions you require and disabling password-based logins for instances launched from your AMI.

Differentiate between Stopping and Terminating an EC2 Instance



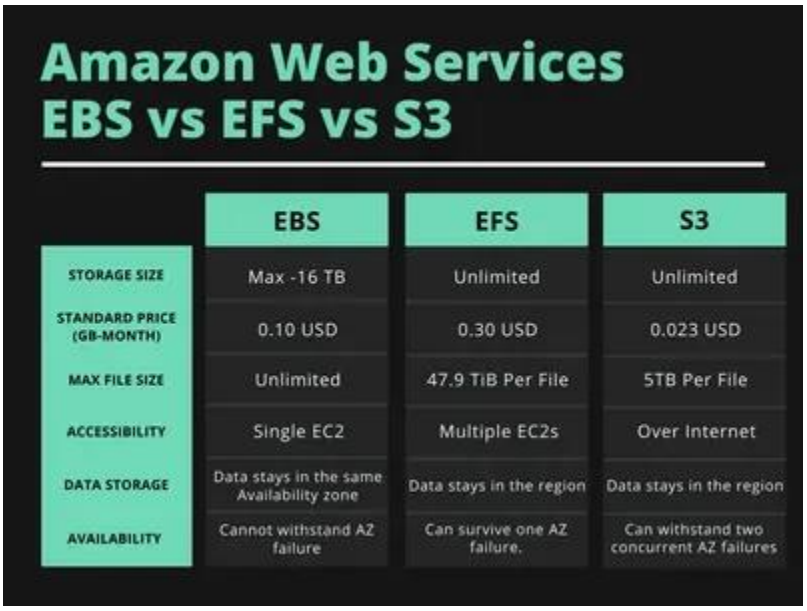
When an Ec2 instance is stopped, a normal shutdown is performed on the instance, whereas when an EC2 instance is terminated, it gets transferred to a stopped state, and then the attached EBS volumes are permanently deleted.

user gain access to a Specific Bucket



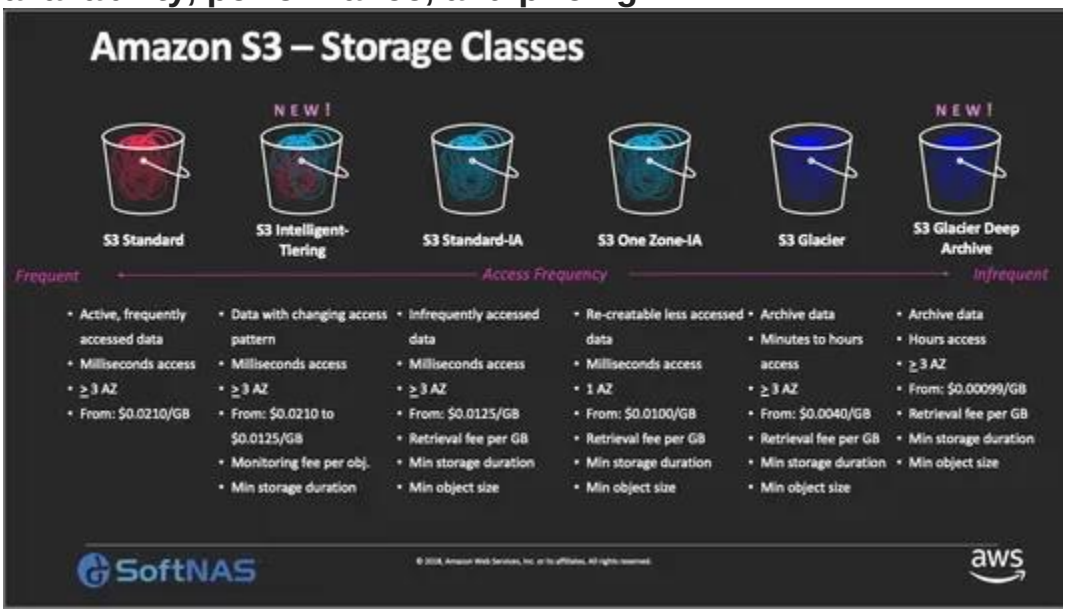
Overall, S3

A few key differences between S3 and EBS



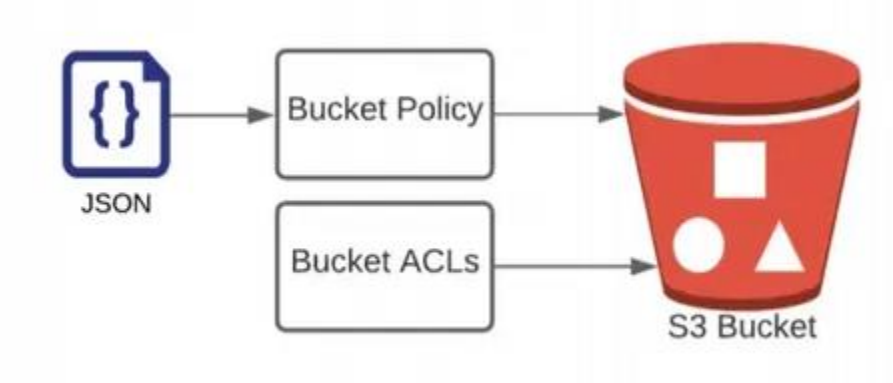
	EBS	EFS	S3
STORAGE SIZE	Max -16 TB	Unlimited	Unlimited
STANDARD PRICE (GB-MONTH)	0.10 USD	0.30 USD	0.023 USD
MAX FILE SIZE	Unlimited	47.9 TiB Per File	5TB Per File
ACCESSIBILITY	Single EC2	Multiple EC2s	Over Internet
DATA STORAGE	Data stays in the same Availability zone	Data stays in the region	Data stays in the region
AVAILABILITY	Cannot withstand AZ failure	Can survive one AZ failure.	Can withstand two concurrent AZ failures

Amazon S3 provides many storage classes with varying durability, availability, performance, and pricing



Amazon S3 Lifecycle Policies

Keep Data Stored in Amazon S3 Safe



1. Bucket Policies: Define rights for one or more buckets using bucket policies. Bucket rules can restrict access and actions.
2. Access Control Lists (ACLs): Define bucket object permissions with ACLs. ACLs can restrict object access and activities.
3. Encryption: You can encrypt data stored in S3 using server-side or client-side encryption. Server-side encryption encrypts data at rest in S3 using encryption keys managed by AWS. Client-side encryption encrypts data before it is uploaded to S3 and requires you to manage the encryption keys.
4. Cross-Origin Resource Sharing (CORS): CORS lets you restrict S3 resource access from non-S3 websites. CORS lets you specify domains and actions for S3 resource access.
5. MFA Delete: S3 buckets can need MFA devices to remove items. This prevents unintended data destruction.
6. Logging and Monitoring: Amazon CloudTrail logs all S3 API calls, and AWS CloudWatch monitors S3 access logs and bucket metrics. This lets you monitor S3 data access and identify unusual activities.