AWS Cloud

-Karan Gupta

Instructor

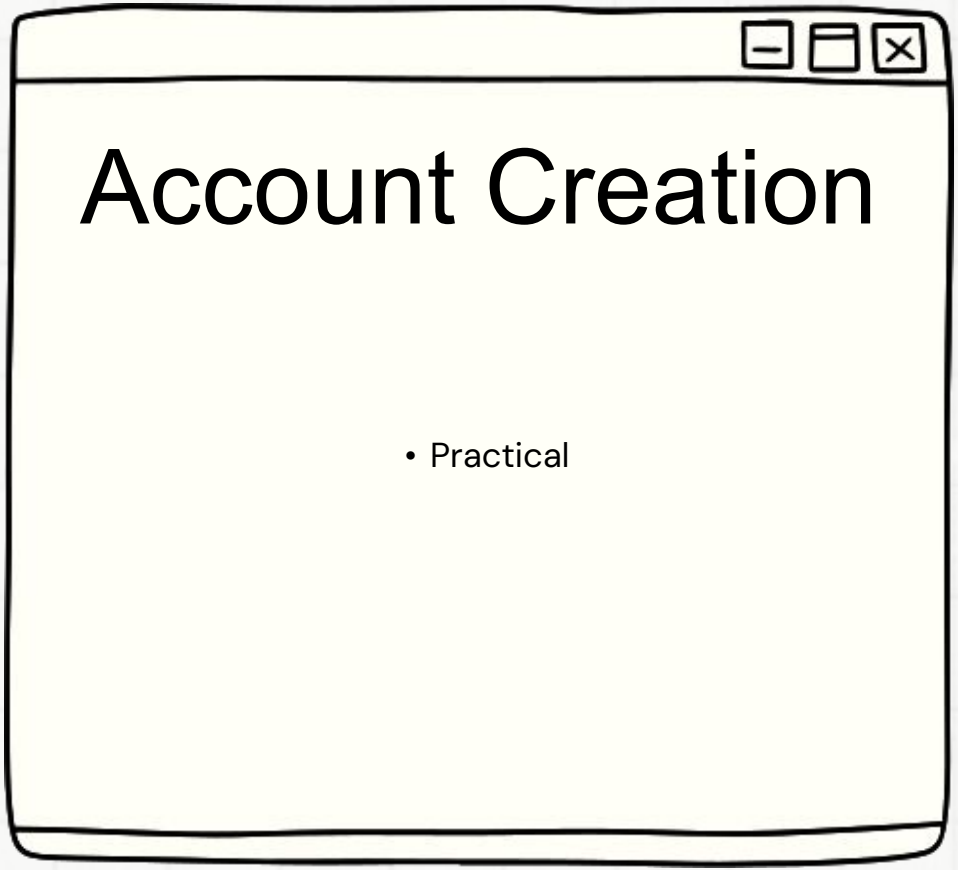
- 5x AWS Certified
- (AWS Certified Solution Architect Professional)
- Worked with MNCs, Startups, Mid-size
- Published Over 10+ Research Papers
- Corporate Trainer

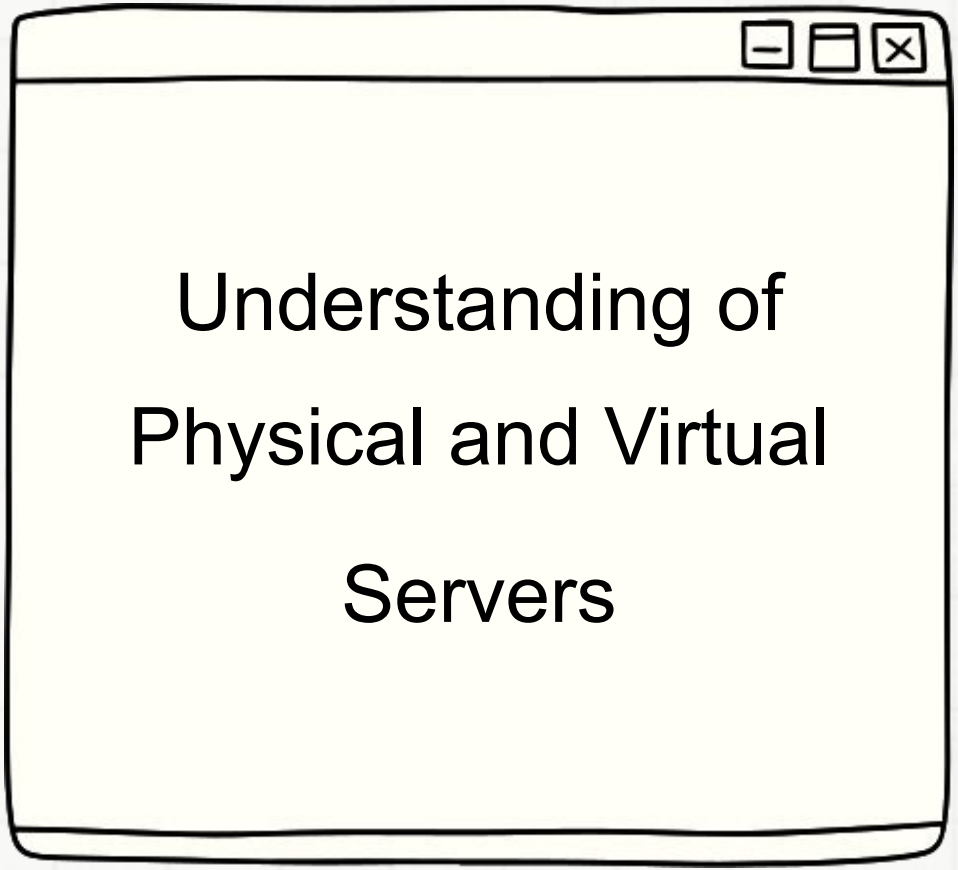
Course Plan

- Prepare for Market
- Q/A
- Interview Based Prep
- AWS certification POV
- Will give practical based scenarios

Account Creation

- 12 months free – Limited
- Will cost if used excessively


Account Creation
• Practical


Understanding of
Physical and Virtual
Servers


aws

What is Server?

- Normal computer or device who hosts website can be considered server.
- Including data centers, offices

Problems in Traditional

- **Cost of physical assets**
- **Requirement of power supply, place, cooling, maintenance**
- **Manpower needed**
- 24*7 monitoring
- **Rent of office, data centers**
- **Issue in scaling**
- **Disaster issues**

Rise of Cloud Computing

- **On demand delivery**
- **Pay as u go**
- **Choose your preference of machine**
- Instant
- **Go global**
- **One click**

Some services you already use

- **Gmail**
- **Hotstar**
- **Netflix**
- Dropbox

Types of Cloud

Public

That is available for everyone.

AWS, AZURE, GCP

Private

- Not exposed to everyone
- Complete control in ur hand
- Security specific

Hybrid

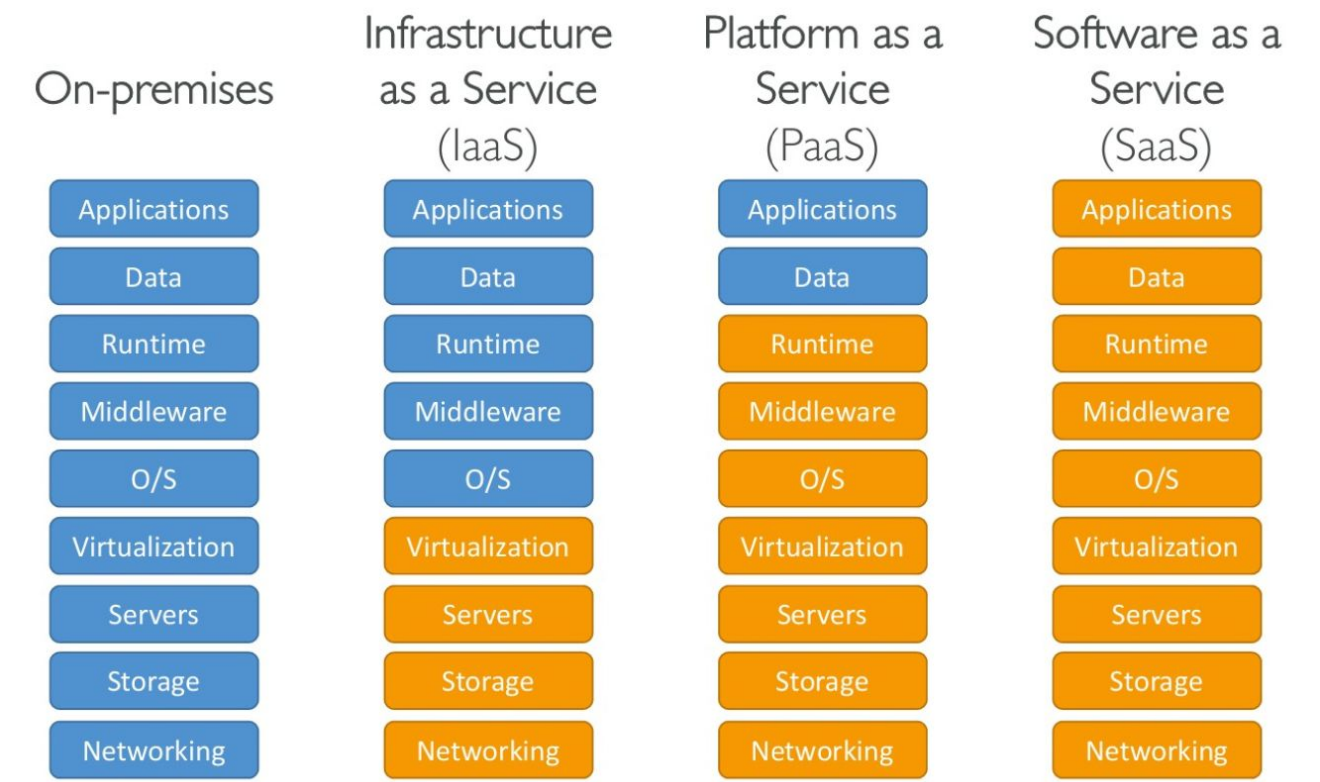
Public + Private

- Sensitive info in private

Need/Benefits of Cloud

- **Flexibility**
- **Scalability**
- **Cost Effective**
- Elasticity
- **High Availability**

Cloud Computing Model



Examples of Each

- IaaS
  - EC2
- PaaS
  - Elastic Beanstalk
- SaaS
  - DropBox, Gmail

Aws Global Infra

- AWS Regions
- AWS AZ
- AWS Data Centers
- Edge Locations

AWS Region

- What are these
- How to select region

AWS AZ

- What are AZ

AWS DC

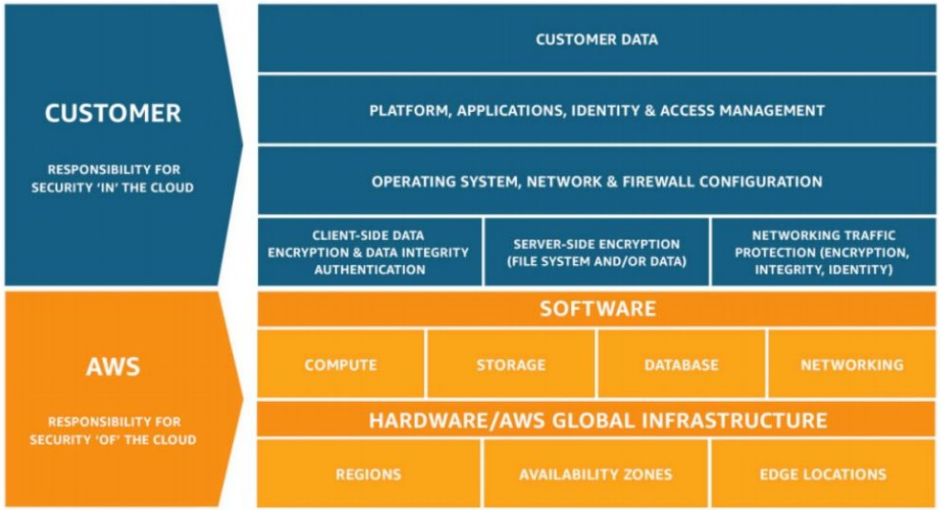
-

Shared Responsibility Model

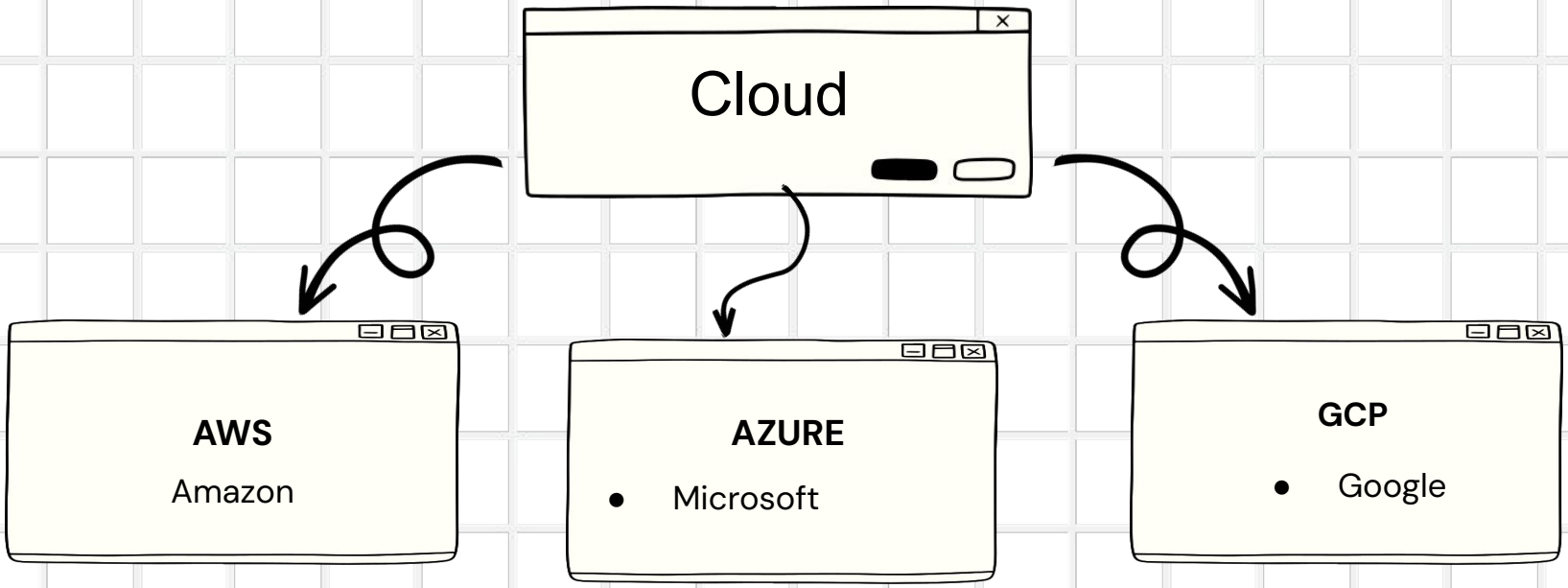
Shared Responsibility Model diagram

CUSTOMER = RESPONSIBILITY FOR THE SECURITY **IN** THE CLOUD

AWS = RESPONSIBILITY FOR THE SECURITY **OF** THE CLOUD



AWS vs Azure vs GCP



AWS vs Azure vs GCP

- https://cloud.google.com/docs/get-started/aws-azure-gcp-service-comparison
- In 2019, AWS – 35$ BILLION revenue
- 47% aws, 22%azure

Pricing

- On aws account
- Cost calculator
- Billing
- budgets
-

Regional vs Global service

- Global –
  - IAM
  - Organisations
  - Route 53
  - ACM
  - Cloudfront

IAM

- Identity and Access Management

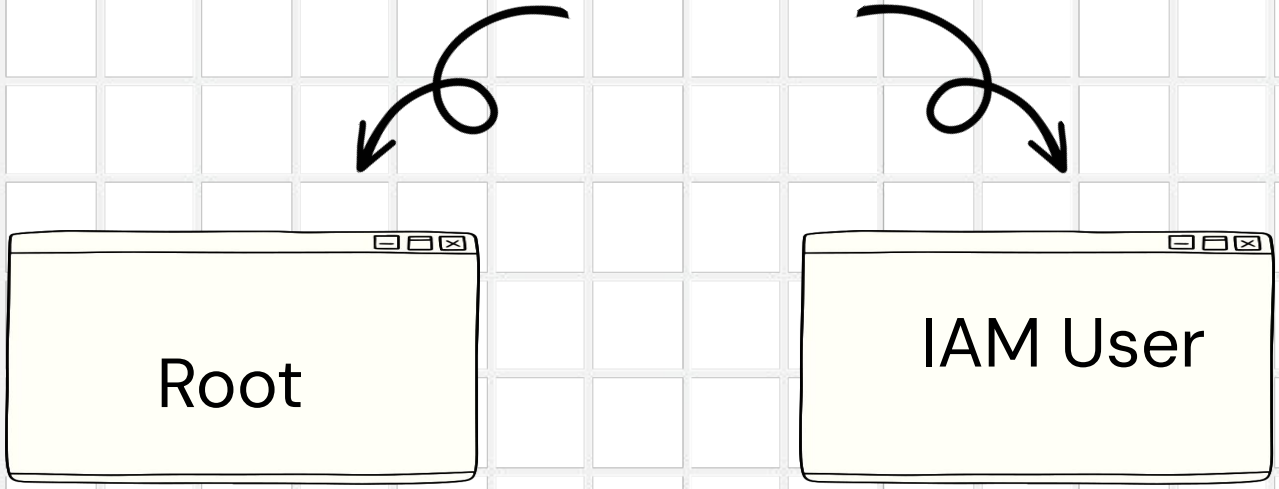
What is IAM

- •Fine-grained control of who can do what
- Eg -user Bob can launch server

IAM Characteristics

- free
- centralized AWS service
- default scope is AWS account
- deny by default

IAM Users



Root User

- Root User
  - the identity used to create AWS account
  - complete access

- Best practices
  - don’t use this account for the everyday
  - setup physical MFA and lock it away
  - don’t use your Amazon.com shopping account

IAM User

- IAM Users
  - an identity with assigned permissions
  - can have username/password access to AWS console
  - can have (secret) key-based access to AWS APIs

- Best Practices
  - rotate credentials (keys, passwords)
  - MFA
  - password policy

IAM Groups

- collection of IAM users
- operates like you'd think
- Best practices
  - manage permissions with groups
  - i.e., assign policies to groups instead of users

IAM Policies

- set of permissions to be granted or denied
- JSON documents
- can be assigned directly to IAM users

```
{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Allow",
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws:s3:::*"
  }, {
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"],
    "Resource":
     "arn:aws:s3:::EXAMPLE-BUCKET-NAME"
  }, {
    "Effect": "Allow",
    "Action": [
      "s3:PutObject",
      "s3:GetObject",
      "s3:DeleteObject" ],
    "Resource":
      "arn:aws:s3:::EXAMPLE-BUCKET-NAME/*"
  } ] }
```

IAM Role

- a 2nd type of AWS identity
  - also has assigned permissions
  - similar to IAM users
- designed to be temporarily assumed
  - e.g. by an EC2 instance
- no associated credentials
- Instance Profiles
  - assigned to EC2 instance
  - container for one or more IAM roles

Best Practice

- **Users** – Create individual users.
- **Permissions** – Grant least privilege.
- **Groups** – Manage permissions with groups.
- **Conditions** – Restrict privileged access further with conditions.
- **Password** – Configure a strong password policy.
- **Rotate** – Rotate security credentials regularly.
- **MFA** – Enable MFA for privileged users.
- **Roles** – Use IAM roles for Amazon EC2 instances.
- **Root** – Reduce or remove use of root.

EC2

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud.

Access reliable, scalable infrastructure on demand. Scale capacity within minutes with SLA commitment of 99.99% availability.

Benefits of EC2

* **Scalability:** Easily **scale up or down** resources based on demand.

* **Flexibility:** Choose from various **instance types** optimized for different workloads (compute, memory, GPU).

* **Cost-effectiveness: Pay-as-you-go** pricing model for only the resources you use.

* **Global Availability:** Available in multiple **AWS regions** worldwide.

Different types of EC2

https://aws.amazon.com/ec2/instance-types/

Size n Conf of EC2

- OS
- CPU
- RAM
- Space
- Network Card
- Firewall

Use Cases of EC2

* Hosting websites and applications.
* Running batch jobs.
* Building and deploying cloud-native applications.
* Setting up development, testing, and staging environments.

Key Pair

- AWS uses public-key cryptography to encrypt and decrypt login information.
- AWS only stores the public key, and the user stores the private key.

Generate Key Pair

1. Open the Amazon EC2 console at http://console.aws.amazon.com/ec2/
2. On the navigation bar select region for the key pair
3. Click **Key Pairs** in the navigation pane to display the list of key pairs associated with the account
4. Click **Create Key Pair**
5. Enter a name for the key pair in the **Key Pair Name** field of the dialog box and click **Create**
6. The private key file, with .pem extension, will automatically be downloaded by the browser.

Steps of creating EC2

Step 1: Sign up for Amazon EC2

Step 2: Create a key pair

Step 3: Launch an Amazon EC2 instance

Step 4: Connect to the instance

Step 5: Customize the instance

Step 6: Terminate instance and delete the volume created

Connecting to EC2

- There are several ways to connect to an EC2 instance once it’s launched.
- **Remote Desktop Connection** is the standard way to connect to Windows instances.
- An **SSH client** (standalone or web-based) is used to connect to Linux instances.

Features of EC2

- Virtual Computing Environments, known as instances
- Preconfigured template for your instance is known as AMI
- Various configuration of CPU, memory, storage and network capacity is Instance type
- Secure login information for your instance using Key pairs

More Features of EC2

- Storage volumes for temporary data that's deleted when hardware fails or terminate your instance, known as instance store volumes
- Persistent storage volumes for your data using Amazon Elastic Block Store (Amazon EBS), known as Amazon EBS volumes
- A firewall that enables you to specify the protocols, ports, and source IP ranges that can reach your instances using security groups
- Metadata, known as tags, that you can create and assign to your Amazon EC2 resources

Intro to SG

A security group in the context of Amazon EC2 is essentially a virtual firewall that controls the traffic for one or more instances.

It acts as a virtual firewall for your EC2 instances to control incoming and outgoing traffic.

Key Points – SG

1. Traffic Control
2. Stateful
3. Flexible rule
4. Layer of Defense
5. Only allowed rules

EC2 Purchasing Option

1. On-Demand
2. Reserved
3. Spot
4. Dedicated

EC2 Purchasing Option

On-Demand

- Charged per second or hour of usage, offering maximum flexibility.
- **No upfront commitment:** Ideal for short-term workloads, testing, or unpredictable usage patterns.
- **Scalability:** Easily scale instances up or down based on real-time needs.
- **Availability:** Guaranteed instance availability within your chosen AWS region.

EC2 Purchasing Option

Reserved

- Offer significant discounts (up to 75%) compared to On-Demand pricing through a prepaid reservation for a specific instance type, region, and term (1 or 3 years).
- **Benefits:**
  - **Significant cost savings** for predictable, sustained workloads.
  - **Guaranteed capacity:** Ensures availability of the specified instance type during your reservation term.

EC2 Purchasing Option

Spot:

- Bid on spare EC2 capacity at significantly lower prices (up to 90% discount) compared to On-Demand Instances. The price fluctuates based on supply and demand.
- **Benefits:**
    - **Lowest cost option** for workloads that can tolerate interruptions.

EBS volume

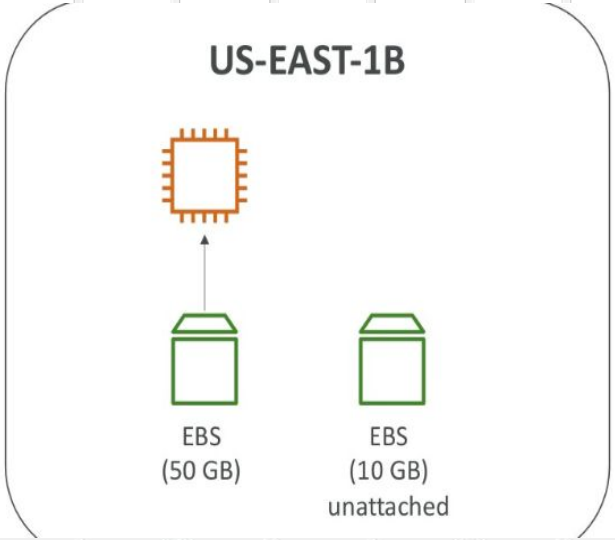
- EBS is drive that you attach when you run the machine/instance.
- Persist even after machine termination
- Can be mounted to one instance at a particular time
- Bound to AZ.

EBS volume- Benefits

- Data Persistence
- Scalability
- Backup and Recovery
- High Availability
- Performance

EBS volume- Key Info

- Restricted to 1 AZ
- It's a N/W drive
- Costly as compared to other Storage services



EBS volume- Attach

- When you just wanna take the add volume which is available in nature.

EBS volume- Detach

- When you just wanna take the backup of data with volume being available then you can detach the volume.

EBS volume- Size Increase

- You can change size of EBS volume
- Only INCREASE possible
- Not decrease
- 1:1

Types of EBS volumes

Amazon EBS provides the following volume types, which differ in performance characteristics and price.

• SSD-backed volumes optimized for transactional workloads involving frequent read/write operations with small I/O size, where the dominant performance attribute is IOPS

• HDD-backed volumes optimized for large streaming workloads where throughput (measured in MiB/s) is a better performance measure than IOPS

Snapshot

- It acts like a frozen image of your data at a specific moment, allowing you to restore your data or create new EBS volumes from that saved state.
- Make a backup of EBS volume at that point of time
- Can be shared among AZ or Region.

Snapshot - Benefits

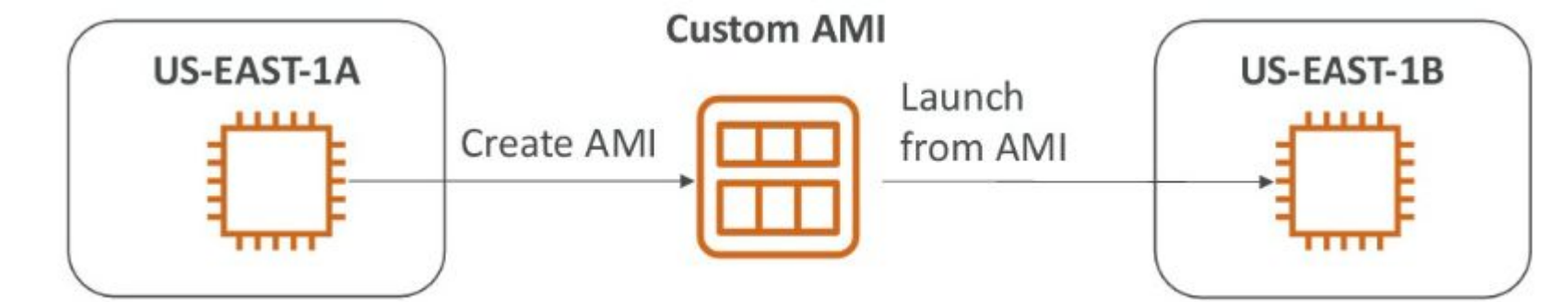
- Data Backup and Recovery
- Disaster Recovery
- Data Archiving
- Data Migration

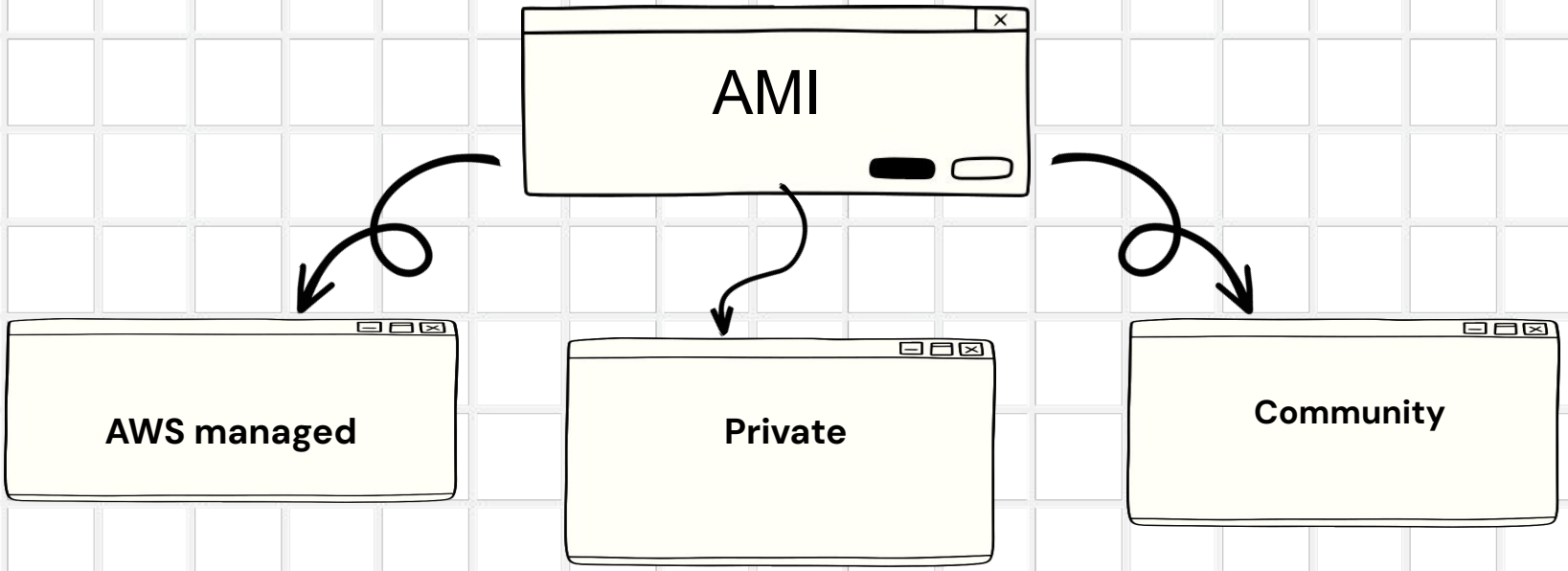
AMI

In Amazon Web Services (AWS), an Amazon Machine Image (AMI) acts as a template for creating virtual servers known as EC2 (Elastic Compute Cloud) instances. It essentially encapsulates the configuration of a server, including the operating system, applications, and settings.

Benefits

- Faster Deployments
- Consistency
- Repeatability
- Improved Manageability




AMI
AWS managed
Private
Community

Finding an Instance type

- Region
- The architecture: 32-bit (i386), 64-bit (x86_64)
- Compute
- Memory
- Storage
- Network performance

Changing the Instance type

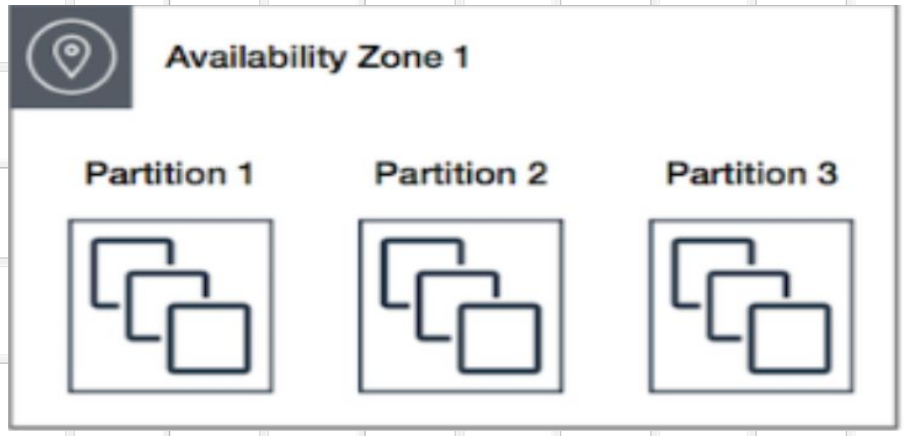
- As your needs change, you might find that your instance is over-utilized or underutilized.
- For example, if your t2.micro instance is too small for its workload, you can change it to another instance type that is appropriate for the workload.
- You might also want to migrate from a previous generation instance type to a current generation instance type to take advantage of some features; for example, support for IPv6.

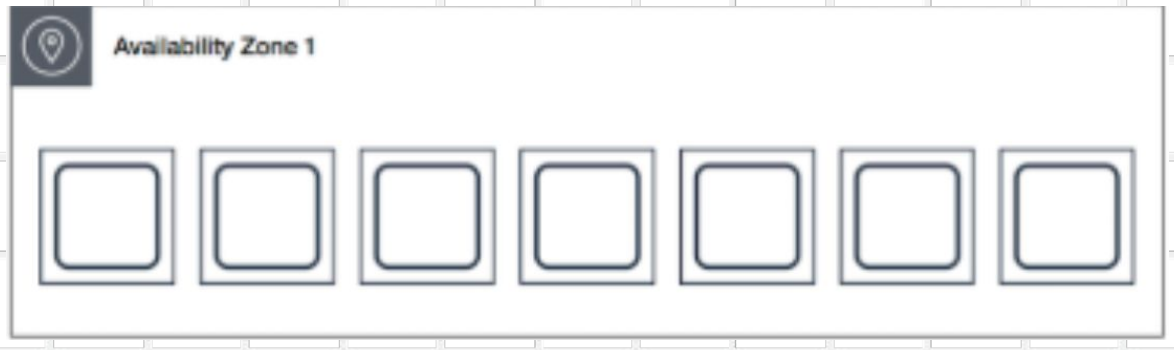
Placement Groups

You can launch or start instances in a placement group, which determines how instances are placed on underlying hardware. When you create a placement group, you can create one of the following strategies for the group:

- Cluster – clusters instances into a low-latency group in a single Availability Zone
- Partition – spreads instances across logical partitions, ensuring that instances in one partition do not share underlying hardware with instances in other partitions
- Spread – spreads instances across distinct underlying hardware

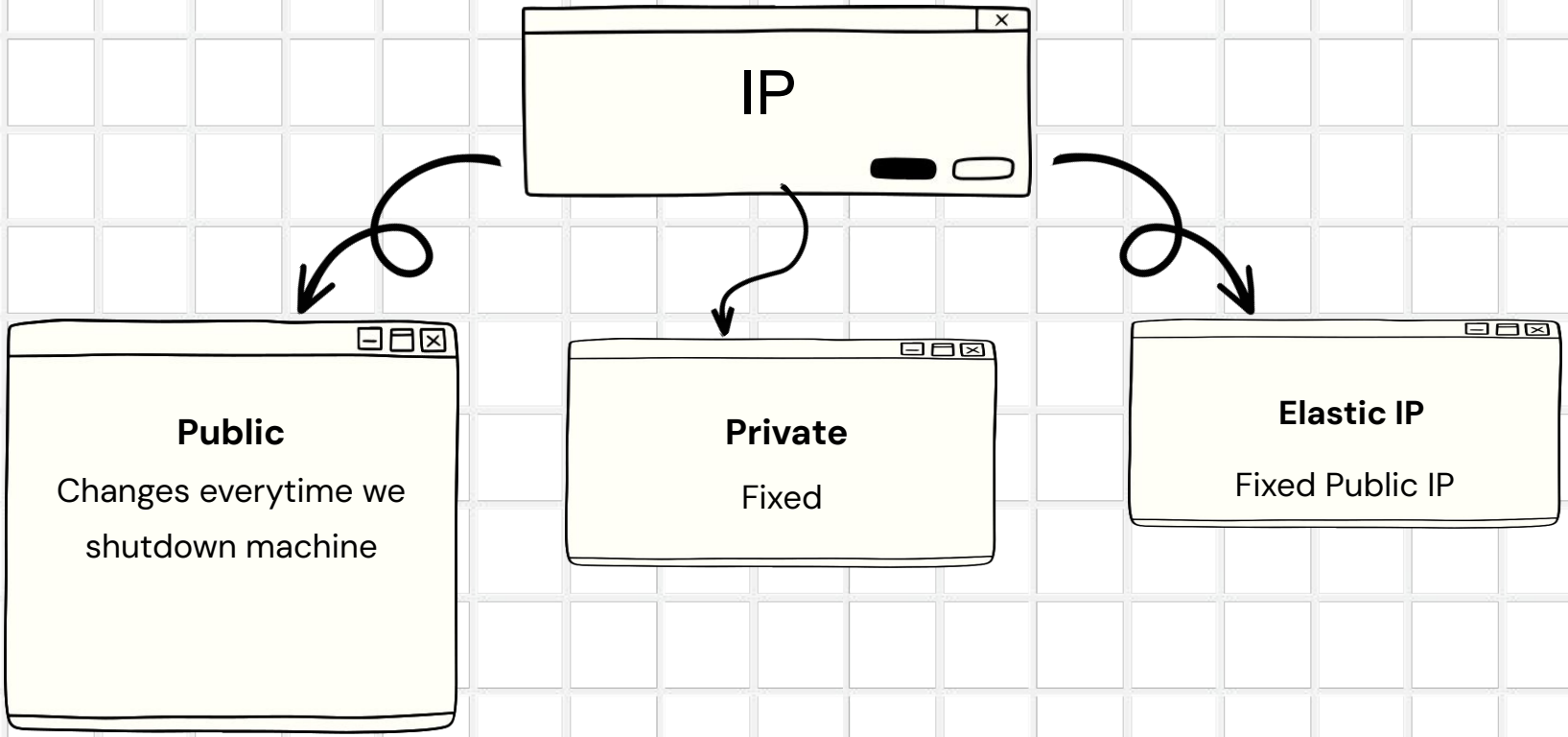

Availability Zone


Availability Zone 1
Partition 1
Partition 2
Partition 3


Availability Zone 1

Other Compute Services

- AWS LAMBDA
- AWS FARGATE


IP
Public
Changes everytime we shutdown machine
Private
Fixed
Elastic IP
Fixed Public IP

Public IP

- A public IP address is an IPv4 address that's reachable from the Internet. You can use public addresses for communication between your instances and the Internet.
- Each instance that receives a public IP address is also given an external DNS hostname; for example,ec2-203-0-113-25.compute-1.amazonaws.com.
- Changes on restart

Private IP

When EC2 instances are launched, the primary IP is assigned a reserved private IP address

- The private IP address stays assigned to the network interface until it is deleted.
- It is not possible to remove or change the private IP address of the primary network interface

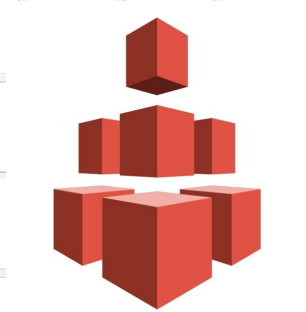
Elastic IP

An Elastic IP address is a static IPv4 address designed for dynamic cloud computing.

- An Elastic IP address is associated with your AWS account.
- With an Elastic IP address, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account.
- An Elastic IP address is a public IPv4 address, which is reachable from the internet.

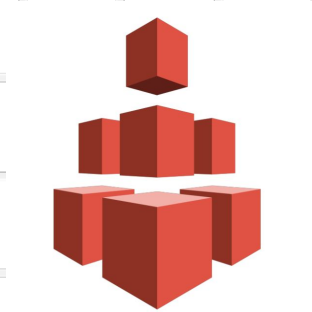
EFS

- Amazon EFS provides a simple, scalable, elastic file system for Linux-based workloads for use with AWS Cloud services and on-premises resources.
- It is built to scale on demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files
- It is designed to provide massively parallel shared access to thousands of Amazon EC2 instances
- It is a fully managed service



EFS

- There is a Standard and an Infrequent Access storage class available with Amazon EFS using Lifecycle Management, files not accessed for 30 days will automatically be moved to a cost-optimized Infrequent Access storage class reducing cost up to 85%
- Amazon EFS is a regional service storing data within and across multiple Availability Zones (AZs) for high availability and durability.



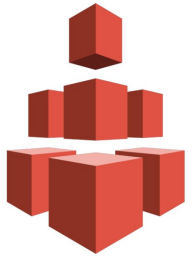
EFS vs EBS

Scalability:

- **EBS**: You can scale EBS volumes by attaching additional volumes to your EC2 instance or using larger volume sizes. However, scaling primarily involves individual instance storage capacity.
- **EFS**: EFS is inherently scalable. You can easily increase or decrease the storage capacity of your file system on demand to accommodate growing data needs.

Availability:

- **EBS**: EBS volumes are designed to be highly available within an Availability Zone. However, they are directly attached to a specific EC2 instance.
- **EFS**: EFS provides higher availability through its distributed architecture across multiple Availability Zones within a region. This ensures that file system access remains available even if a single Availability Zone encounters an outage.



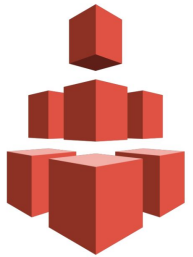
EFS vs EBS

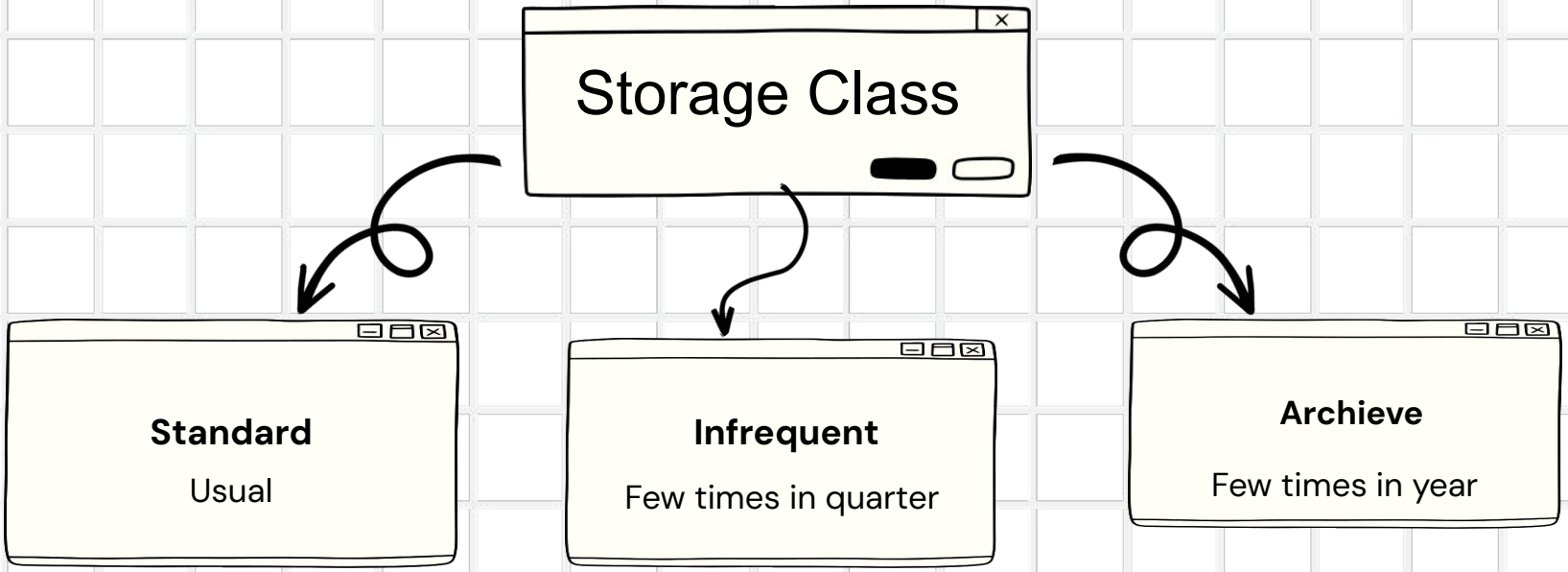
Cost:

- **EBS:** EBS billing is based on the provisioned storage size (per GiB per month) and the type of volume (e.g., magnetic, SSD, NVMe SSD).
- **EFS:** EFS billing is based on the amount of data stored (per GiB per month) and the number of concurrent file operations (IOPS).

Performance:

- **EBS:** EBS offers high performance, making it suitable for applications requiring fast storage access, such as databases or applications working with large datasets.
- **EFS:** While EFS provides good performance, it might not match the raw speed of EBS due to its distributed nature. However, EFS scales well for concurrent access from multiple instances.



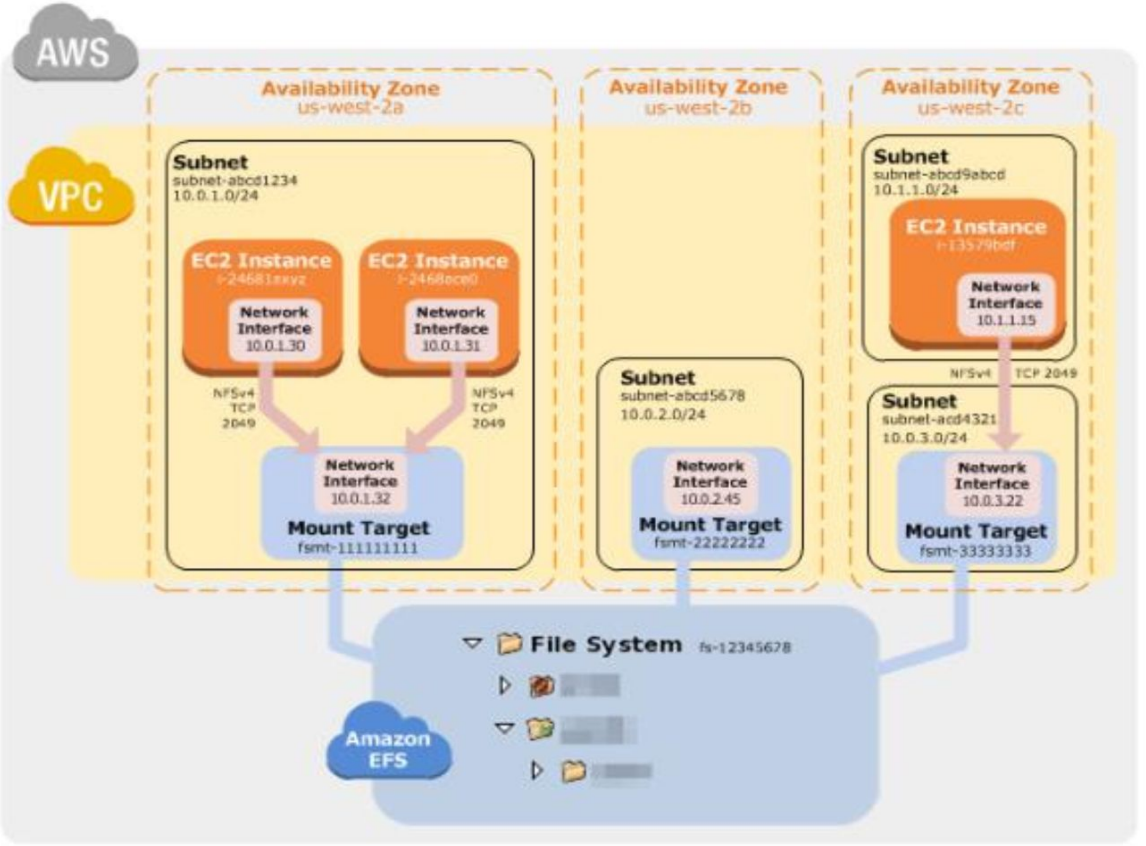

Storage Class
Standard
Usual
Infrequent
Few times in quarter
Archieve
Few times in year

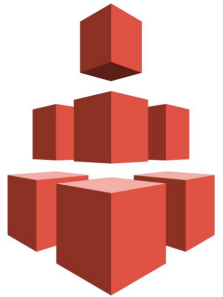
EFS

- **Important**:

  Amazon EFS is not supported on Windows instances.

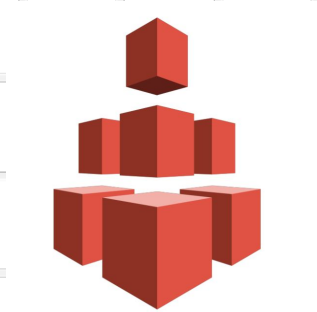
EFS


AWS
Availability Zone
us-west-2a
Availability Zone
us-west-2b
Availability Zone
us-west-2c
VPC
Subnet
subnet-abcd1234
10.0.1.0/24
EC2 Instance
Network Interface
10.0.1.30
EC2 Instance
Network Interface
10.0.1.31
NFSv4
TCP
2049
NFSv4
TCP
2049
Network Interface
10.0.1.32
Mount Target
fsmt-111111111
Subnet
subnet-abcd5678
10.0.2.0/24
Network Interface
10.0.2.45
Mount Target
fsmt-22222222
Subnet
subnet-abcd9abcd
10.1.1.0/24
EC2 Instance
Network Interface
10.1.1.15
NFSv4
TCP 2049
Subnet
subnet-acd4321
10.0.3.0/24
Network Interface
10.0.3.22
Mount Target
fsmt-33333333
File System
fs-12345678
Amazon
EFS



EFS-Benefits

- Dynamic elasticity
- Scalable performance
- Shared file storage
- Fully managed
- Cost effective – pay for what you use (no upfront capacity planning)
- Pricing



EFS–Use Cases

Amazon EFS is designed to meet the performance needs of the following use cases.

- Big Data and Analytics
- Media Processing Workflows
- Content Management and Web Serving
- Home Directories

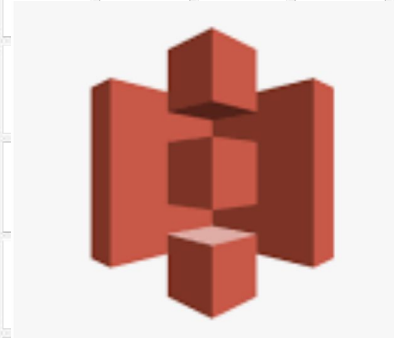
EFS–Use Cases

Amazon EFS is designed to meet the performance needs of the following use cases.

- Big Data and Analytics
- Media Processing Workflows
- Content Management and Web Serving
- Home Directories

S3

- Amazon Simple Storage Service is storage for the Internet
- 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.



S3– Advantages

Amazon S3 is intentionally built with a minimal feature set that focuses on simplicity and robustness

- Creating buckets – Create and name a bucket that stores data. Buckets are the fundamental container in Amazon S3 for data storage.
- Storing data – Store an infinite amount of data in a bucket. Upload as many objects as you like into an Amazon S3 bucket. Each object can contain up to 5 TB of data.

S3- Advantages Cont.

- **Downloading data** – Download your data or enable others to do so. Download your data anytime you like, or allow others to do the same.

- **Permissions** – Grant or deny access to others who want to upload or download data into your Amazon S3 bucket.

S3– Use Cases

- Backup and Storage
- Disaster Recovery
- Archive
- Application Hosting
- Static Website

S3- Concepts

Buckets

- To upload your data (photos, videos, documents etc.) to Amazon S3, you must first create an S3 bucket in one of the AWS Regions.
- A bucket is a region specific
- A bucket is a container for objects stored in Amazon S3.

S3- Concepts Cont.

- Every object is contained in a bucket.
- By default, you can create up to 100 buckets in each of your AWS accounts. If you need more buckets, you can increase your account bucket limit to a maximum of 1,000 buckets by submitting a service limit increase.
- For example, if the object named photos/puppy.jpg is stored in the john bucket in the US West (Oregon) Region, then it is addressable using the URL https://john.s3.us-west-2.amazonaws.com/photos/puppy.jpg

S3- Buckets

- For Bucket name to be created, follow the naming guidelines

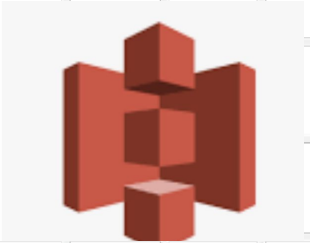
• Bucket name should be globally unique and the namespace is shared in all accounts. This means that after a bucket is created, the name of that bucket cannot be used by another AWS account in any AWS Region until the bucket is deleted.

• Once created it cannot be changed

S3- Buckets

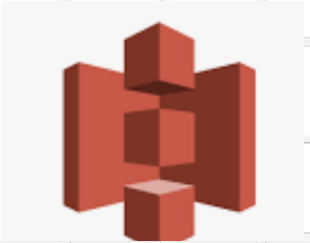
- Bucket names must be at least 3 and no more than 63 characters long.
- Bucket names must not contain uppercase characters or underscores.
- Bucket names must start with a lowercase letter or number.
- Bucket names must not be formatted as an IP address (for example, 192.168.5.4).
- After you create the bucket, you cannot change the name, so choose wisely.
- Choose a bucket name that reflects the objects in the bucket because the bucket name is visible in the URL that points to the objects that you're going to put in your bucket.

S3– Regions



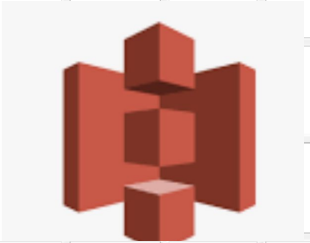
- You can choose the geographical AWS Region where Amazon S3 will store the buckets that you create.
- You might choose a Region to optimize latency, minimize costs, or address regulatory requirements.
- Objects stored in a Region never leave the Region unless you explicitly transfer them to another Region.
- For example, objects stored in the Europe (Ireland) Region never leave it.

S3- Objects



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

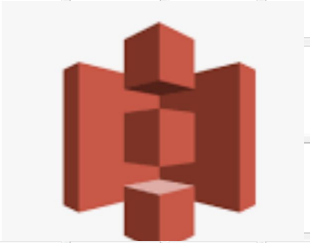
S3- Objects Cont.



An object consists of the following:

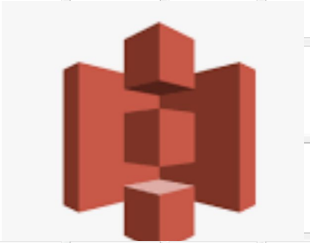
- Key – The name that you assign to an object.
- Version ID – Within a bucket, a key and version ID uniquely identify an object.
- Value – The content that you are storing.
- Metadata – A set of name-value pairs with which you can store information regarding the object.

S3– Objects Versioning



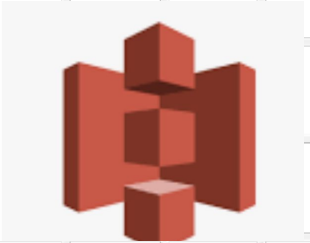
- When you re-upload the same object name in a bucket, it replaces the whole object
- You can use versioning to keep multiple versions of an object in one bucket.
- For example, you could store my-image.jpg (version 1) and my-image.jpg (version 2) in a single bucket.
- Versioning protects you from the consequences of unintended overwrites and deletions.
- You must explicitly enable versioning on your bucket. By default, versioning is disabled.

Objects Versioning Cont.



- Regardless of whether you have enabled versioning, each object in your bucket has a version ID.
- If you have not enabled versioning, Amazon S3 sets the value of the version ID to null. If you have enabled versioning, Amazon S3 assigns a unique version ID value for the object.
- This functionality prevents you from accidentally overwriting or deleting objects and affords you the opportunity to retrieve a previous version of an object.

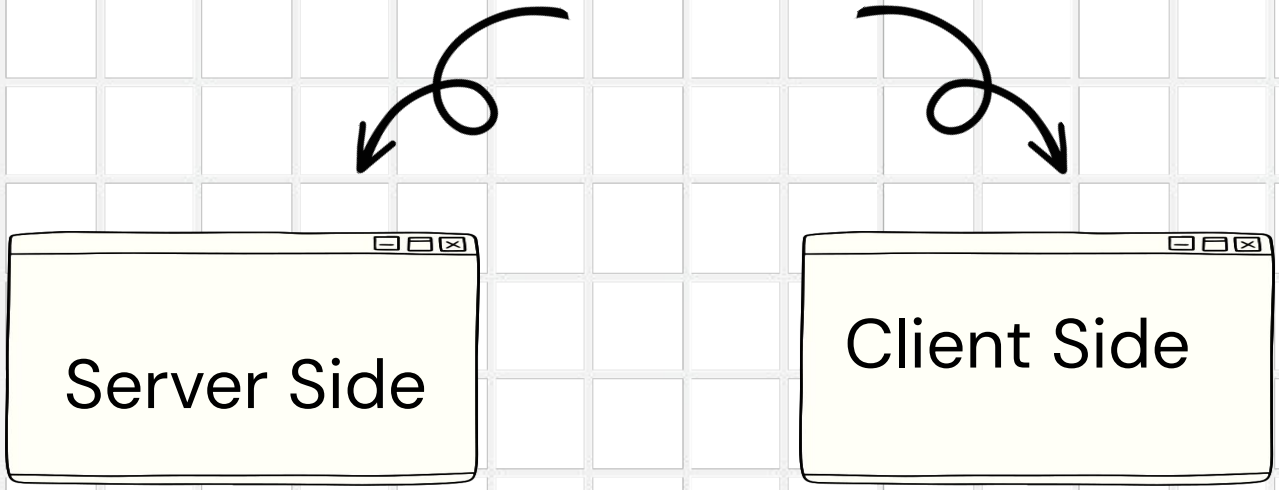
S3 logs



Server Access Logging

- 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.
- 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.
- Both the source and target S3 buckets must be owned by the same AWS account, and the S3 buckets must both be in the same Region.

S3 Encryption



S3 Encryption

Data protection refers to protecting data while in-transit (as it travels to ar from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You have the following options for protecting data at rest in Amazon S3:

- Server-Side Encryption – Request Amazon S3 to encrypt your object before saving it on disks in its data centers and then decrypt it when you download the objects.
- Client-Side Encryption – Encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

S3 Server Side Encryption

Server Side Encryption

- Server-side encryption is the encryption of data at its destination by the application or service that receives it.
- Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it.
- As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects.

SSE-S3

Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

- When you use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3), each object is encrypted with a unique key.
- As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates.

SSE-KMS

Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS)

- Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS) is similar to SSE-S3, but with some additional benefits and charges for using this service.

SSE-KMS

Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS)

- Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS) is similar to SSE-S3, but with some additional benefits and charges for using this service.

SSE-C

Server-Side Encryption with Customer-Provided Keys (SSE-C)

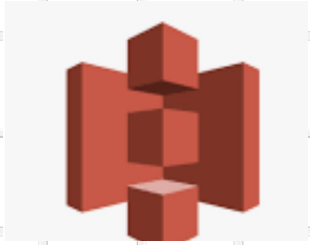
- With Server-Side Encryption with Customer-Provided Keys (SSE-C), you manage the encryption keys and Amazon S3 manages the encryption, as it writes to disks, and decryption, when you access your objects.

Client Side Encryption

Client-side encryption is the act of encrypting data before sending it to Amazon S3. To enable client-side encryption, you have the following options:

- Use a customer master key (CMK) stored in AWS Key Management Service (AWS KMS).
- Use a master key you store within your application.

Static Website Hosting



- You can host a static website on Amazon S3. On a static website, individual web pages include static content.
- To host a static website, you configure an Amazon S3 bucket for website hosting and then upload your website content to the bucket.
- This bucket must have public read access. It is intentional that everyone in the world will have read access to this bucket.

Static Website Hosting

- Depending on your Region, Amazon S3 website endpoints follow one of these two formats:

- http://bucket-name.s3-website.Region.amazonaws.com
- http://bucket-name.s3-website-Region.amazonaws.com
- This above URL will return the default index document that you configured for the website.

Storage Class

- Each object in Amazon S3 has a storage class associated with it.
- Amazon S3 offers a range of storage classes for the objects that you store.
- You choose a class depending on your use case scenario and performance access requirements. All of these storage classes offer high durability.

Storage Classes– Frequent

For performance-sensitive use cases (those that require millisecond access time) and frequently accessed data, Amazon S3 provides the following storage class

- **Standard**—The default storage class. If you don't specify the storage class when you upload an object, Amazon S3 assigns the Standard storage class.

Storage Classes- Infrequent

- **The Standard_IA and Onezone_IA** storage classes are designed for long-lived and infrequently accessed data
- Standard_IA and Onezone_IA objects are available for millisecond access (similar to the Standard storage class)
- Amazon S3 charges a retrieval fee for these objects, so they are most suitable for infrequently accessed data.
- The Standard_IA and Onezone_IA storage classes are suitable for objects larger than 128KB that you plan to store for at least 30 days. If an object is less than 128 KB, Amazon S3 charges you for 128 KB.
- Onezone_IA - Amazon S3 stores the object data in only one Availability Zone, which makes it less expensive than Standard_IA

Storage Classes- Archive

-The Glacier and Deep Archive storage classes are designed for low-cost data archiving

Glacier

- Long-term data archiving with retrieval times ranging from minutes to hours
- It has minimum storage duration period of 90 days
- If you have deleted, overwritten, or transitioned to a different storage class an object before the 90-day minimum, you are charged for 90 days.

Storage Classes- Archive

Glacier Deep Archive

- Archiving rarely accessed data with a default retrieval time of 12 hours
- It has minimum storage duration period of 180 days
- If you have deleted, overwritten, or transitioned to a different storage class an object

before the 180-day minimum, you are charged for 180 days.

Storage Classes- Auto Optimizes

- The Intelligent_Tiering storage class is designed to optimize storage costs by automatically moving data to the most cost-effective storage access tier, without performance impact or operational overhead.
- Intelligent_Tiering delivers automatic cost savings by moving data on a granular object level between two access tiers, when access patterns change
- Frequent access tier
- Lower-cost infrequent access tier

Object Lifecycle

- To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle.
- A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects.

There are two types of actions
Transition actions—Define when objects transition to another storage class.
Expiration actions—Define when objects expire. Amazon S3 deletes expired objects on yourbehalf.

Replication

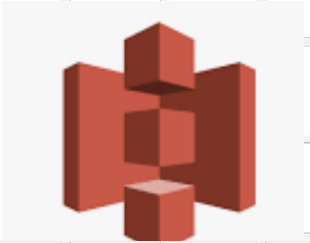
- Replication enables automatic, asynchronous copying of objects across Amazon S3 buckets.
- Buckets that are configured for object replication can be owned by the same AWS account or by different accounts.
- You can copy objects between different AWS Regions or within the same Region.

Types of Object Replication

You can replicate objects between different AWS Regions or within the same AWS Region.

1. Cross-Region replication (CRR) is used to copy objects across Amazon S3 buckets in different AWS Regions.
2. Same-Region replication (SRR) is used to copy objects across Amazon S3 buckets in the same AWS Region.

S3 Delete Bucket



- You can delete the objects individually. Or you can empty a bucket, which deletes all the objects in the bucket without deleting the bucket.
- You can also delete a bucket and all the objects contained in the bucket.
- If you want to use the same bucket, don’t delete the bucket, can empty the bucket and keep it.
- After you delete the bucket, It is available for re-use, but the name might not be available for you to reuse for various reasons. For example, it might take some time before the name can be reused, and some other account could create a bucket with that name before you do.

VPC

• Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined.

• A virtual private cloud (VPC) is a virtual network dedicated to your AWS account.

• It is logically isolated from other virtual networks in the AWS Cloud.

• You can launch your AWS resources, such as Amazon EC2 instances, into your VPC.

VPC

- You can specify an IP address range for the VPC, add subnets, associate security groups, and configure route tables.
- A VPC spans all the Availability Zones in the region.
- After creating a VPC, you can add one or more subnets in each Availability Zone.
- Each subnet must reside entirely within one Availability Zone and cannot span zones.

VPC

- You can specify an IP address range for the VPC, add subnets, associate security groups, and configure route tables.
- A VPC spans all the Availability Zones in the region.
- After creating a VPC, you can add one or more subnets in each Availability Zone.
- Each subnet must reside entirely within one Availability Zone and cannot span zones.

Default vs Custom VPC

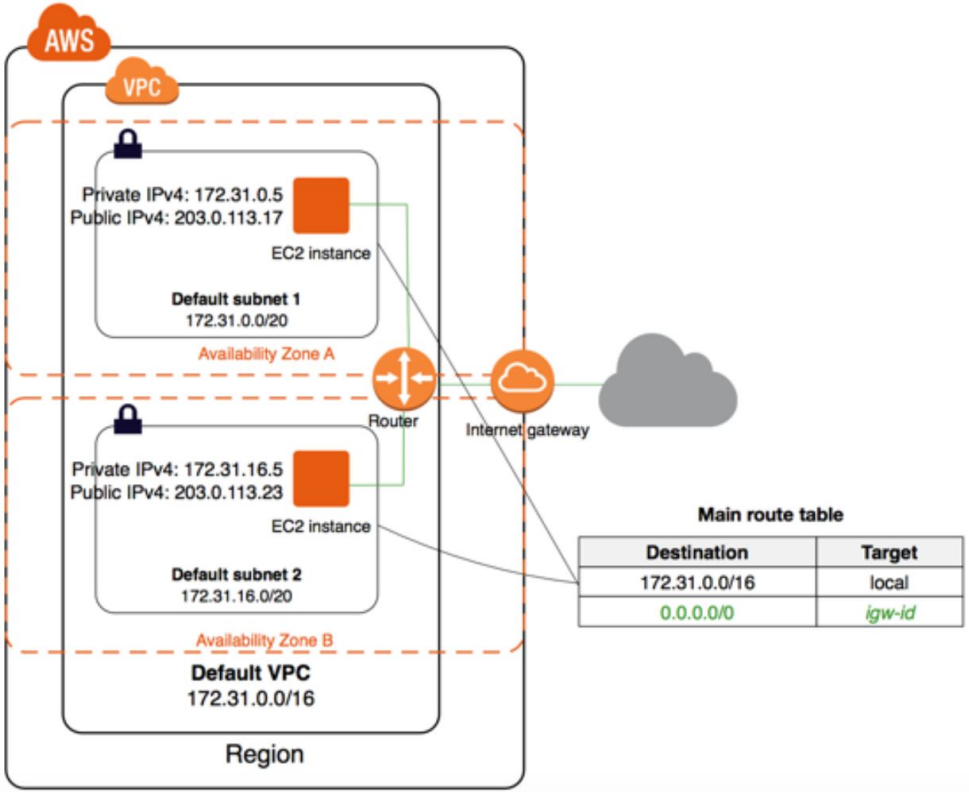
• If your account supports the EC2-VPC platform only, it comes with a default VPC that has a default subnet in each Availability Zone.

• A default VPC has the benefits of the advanced features provided by EC2-VPC, and is ready for you to use. If you have a default VPC and don't specify a subnet when you launch an instance, the instance is launched into your default VPC. You can launch instances into your default VPC without needing to know anything about Amazon VPC.

• Regardless of which platforms your account supports, you can create your own VPC, and configure it as you need. This is known as a non-default VPC. Subnets that you create in your non-default VPC and additional subnets that you create in your default VPC are called non-default subnets.

Accessing the Internet

- Your default VPC includes an internet gateway, and each default subnet is a public subnet. Each instance that you launch into a default subnet has a private IPv4 address and a public IPv4 address. These instances can communicate with the internet through the internet gateway.



VPC and Subnet

- When you create a VPC, you must specify an IPv4 CIDR block for the VPC
- The allowed block size is between a /16 netmask (65,536 IP addresses) and /28 netmask (16 IP addresses)

- The CIDR block of a subnet can be the same as the CIDR block for the VPC, or a subset of the CIDR block for the VPC (for multiple subnets)

- The allowed block size for a subnet is between a /28 netmask and /16 netmask. If you create more than one subnet in a VPC, the CIDR blocks of the subnets cannot overlap.

Reserved IPs

- The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use, and cannot be assigned to an instance.
- For example, in a subnet with CIDR block 10.0.0.0/24, the following five IP addresses are reserved:

10.0.0.0: Network address.
10.0.0.1: Reserved by AWS for the VPC router.
10.0.0.2: Reserved by AWS for the IP address of the DNS server
10.0.0.3: Reserved by AWS for future use.
10.0.0.255: Network broadcast address. We do not support broadcast in a VPC

Public & Private Subnet

The instances in the public subnet can send outbound traffic directly to the Internet, whereas the instances in the private subnet can't. Instead, the instances in the private subnet can access the Internet by using a network address translation (NAT) gateway that resides in the public subnet.

VPC Flow Logs

- VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC.
- Flow log data can be published to Amazon CloudWatch Logs or Amazon S3
- You can create a flow log for a VPC, a subnet

NACl

- A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets
- Each subnet in your VPC must be associated with a network ACL
- You can associate a network ACL with multiple subnets
- A subnet can be associated with only one network ACL at a time
- A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic
- Network ACLs are stateless

NACl

Inbound					
Rule #	**Type**	**Protocol**	**Port Range**	**Source**	**Allow/Deny**
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY
Outbound					
Rule #	**Type**	**Protocol**	**Port Range**	**Destination**	**Allow/Deny**
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

Route Tables

- A route table contains a set of rules, called routes, that are used to determine where network traffic from your subnet or gateway is directed.
- Main route table—The route table that automatically comes with your VPC. It controls the routing for all subnets that are not explicitly associated with any other route table.
- Custom route table—A route table that you create for your VPC.
- Each subnet in your VPC must be associated with a route table
- A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same subnet route table

Internet Gateway

- An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet.
- It therefore imposes no availability risks or bandwidth constraints on your network traffic.

NAT

- You can use a NAT device to enable instances in a private subnet to connect to the internet (for example, for software updates) or other AWS services, but prevent the internet from initiating connections with the instances. A NAT device forwards traffic from the instances in the private subnet to the internet or other AWS services, and then sends the response back to the instances.
- AWS offers two kinds of NAT devices
- NAT Gateway : You are charged for creating and using a NAT gateway in your account. NAT gateway hourly usage and data processing rates apply.
- NAT Instance - A NAT instance is launched from a NAT AMI

VPC Peering

- A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately.
- Instances in either VPC can communicate with each other as if they are within the same network.
- You can create a VPC peering connection between your own VPCs, with a VPC in another
AWS account, or with a VPC in a different AWS Region.
- AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor an VPN connection, and does not rely on a separate piece of physical hardware.
- There is no single point of failure for communication or a bandwidth bottleneck.

Direct Connect

• AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS.

• Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.