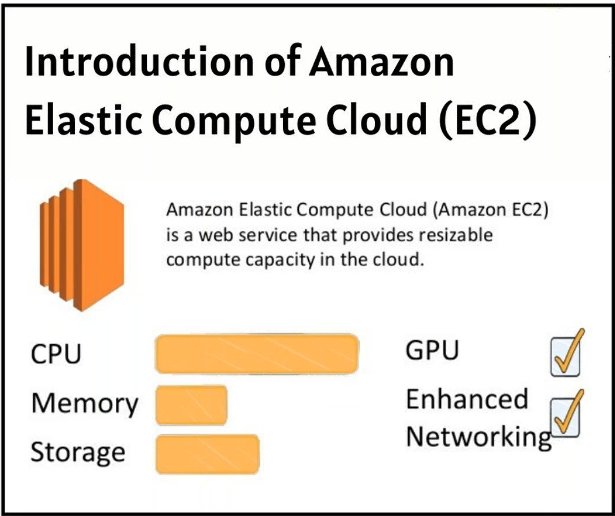
EC2:Elastic Cloud Computing



* Ec2 is a part of Amazon web services of cloud computing platform
* Aws allows users to rent virtual computers on which to run their own computer application
* Ec2 provides scalable computing in Aws

**Components of EC2 Are**

* Instances
* AMI’S
* Volumes
* Snapshots
* Elastic IP’s
* Load Balancer
* Auto Scaling



* Ec2 Instance: An Amazon EC2 instance is **a virtual server in Amazon's Elastic Compute Cloud (EC2) for running applications on the Amazon Web Services (AWS) infrastructure**
* By using AWS EC2 helps users to avoid the investment in hardware up front, so the user can deploy and develop applications easier.
* It is used to launch many virtual servers, configure networking and security, and managing storage.
* Launching an ec2 instance we 7steps to follow those are:

step1:AMI

step2:instance type(t2 micro)

step3:configure instance

In realtime we have to use protect against accendental termination

Tenancy provide more security,if we want to enable it we have to pay double charges

in this we have 3 types shared,dedicate,dedicated host

step4:storage

we can increase size

volume type -different drives are available(ssd)

delete on termination-in real time we need to uncheck

step5:adding tags

step6:configure securty group

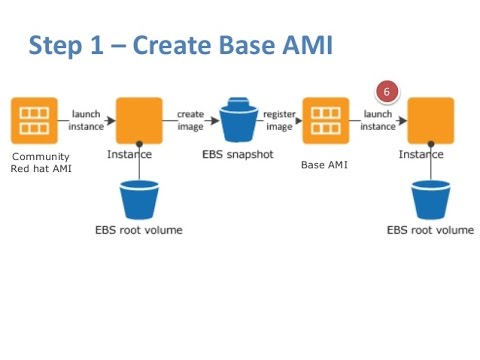
in real time we use existing security group

step7:review and lauch

before laucing we will see all the details what we have given in previous steps

AMI:Amazon Machine Image

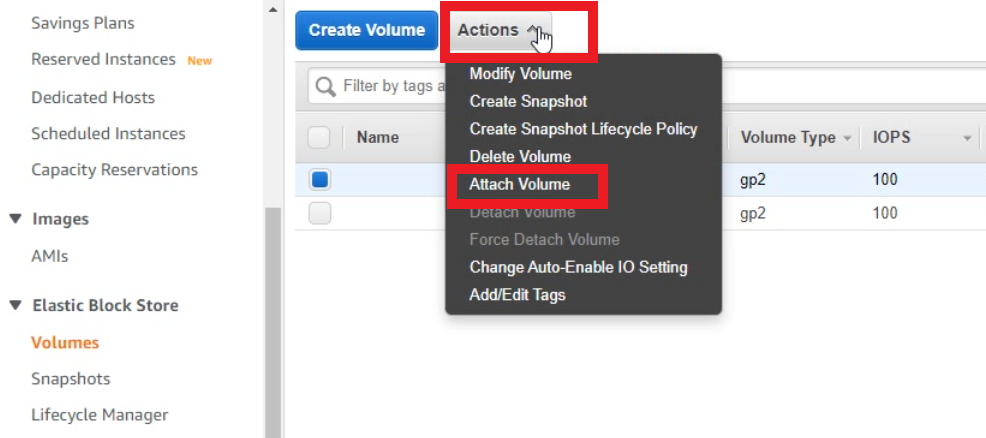
* Ami is a master image of virtual server in aws
* It is a blueprint of ec2 instance that means what we have done in ec2 instance that same data will reflect into the AMI Image



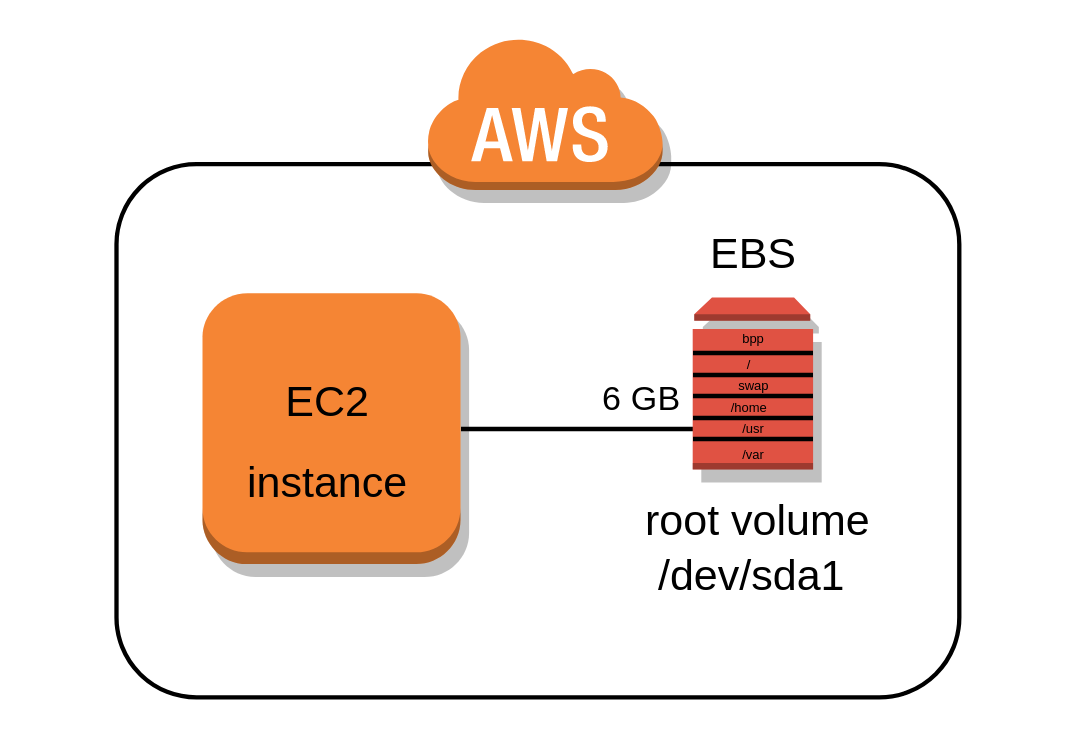
* AMI used whenever we want to backup the data of terminating ec2 instance
* We need to use AMI to backup the data in our ec2 instance what we have deployed
* After the project we will terminate the instance but we need the data what we have done on that case we use ami because we want to terminate instance otherwise we will get charges for that so we use ami back

Volumes:It is nothing but Storage

* Ec2 volumes called as Elastic Block Storage
* EC2 Volumes are essentially disk images that can be mounted on any system running on EC2, and continue to exist even if the system they were attached to is deleted.
* Whenever we create an instance we get default volume with default storage.If we want extra storage we will create volume and attach that volume to the instance

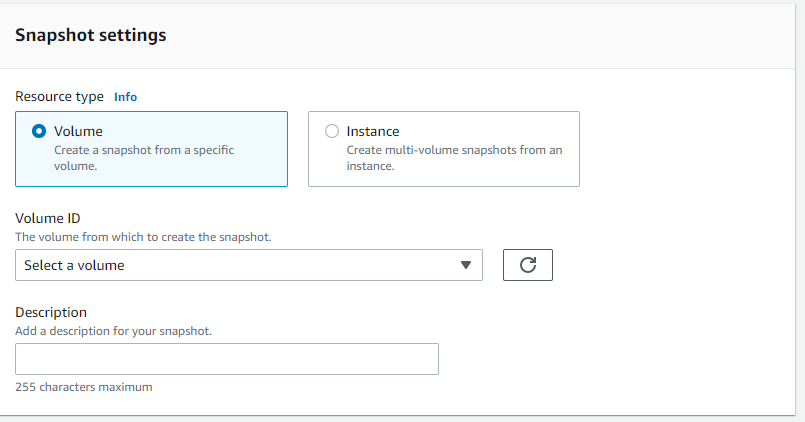


* If we delete instance also the data is in volume
* Volume is also called as backup of ec2 instance

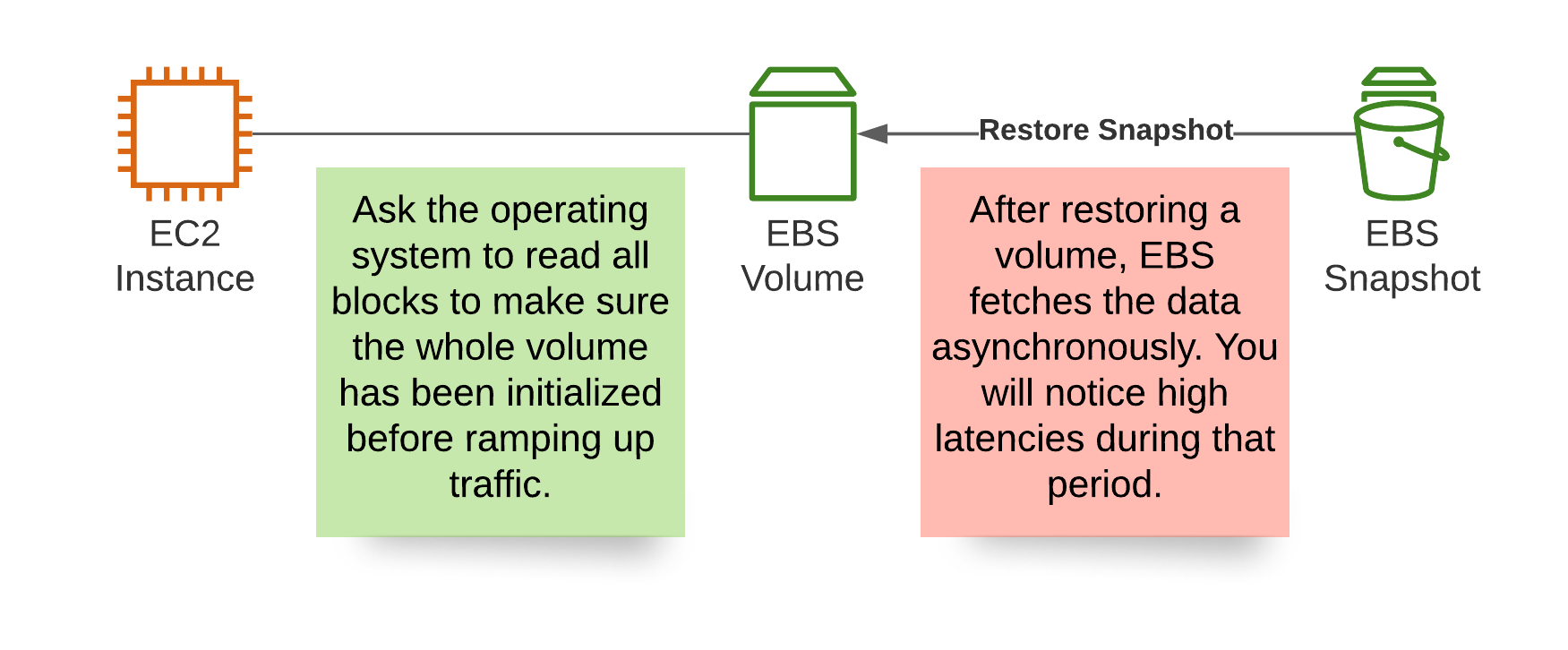


Snapshot:

* A snapshot is taken for all the volumes that are attached to the instance.
* Snapshot is nothing backup of ec2 instance and also backup of volume



* If we want to complete ec2 instance backup we have to select instance and give instance id for ceating snapshot
* If we want only our created volume backup we have to select volume and give volume id for creating snapshot

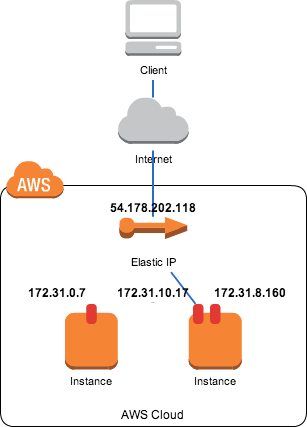


Elastic IP: It is also called as static ip

* When we create an ec2 instance we will get two ip’s public ip and private ip
* Public ip is called as dynamic ip
* Private ip is called as static ip

Use of Elastic ip:

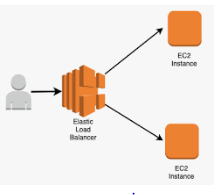
* Whenever we start and stop our ec2 instance public ip will be changed
* To overcome that we will create an elastic ip and assign that ip to ec2 instance
* After completion of our ec2 instance we have to disassociate that elastic ip and release that elastic ip because we get charges for that it is not free of cost



Load Blancing:

A load blancer distributes incoming application traffic across multiple ec2 instances in multiple available zones

* It monitors the health of its registered targets, and routes traffic only to the healthy targets.



Use of load blancer:

lets you evenly distribute network traffic to prevent failure caused by overloading a particular resource

Purpose of load blancer:

To prevent any single server from getting overloaded and possible breaking down

**Target Groups**

Target groups are used to direct traffic from a load balancer to a specific destination

Types of load blancers:

* Application load blancer

It allows a developers to configure and route incoming end-user traffic to application based in the aws cloud

* Network load blancer

It distributes your incoming traffic across multiple targets such as ec2 instances,containers and ip address in one or more available zones

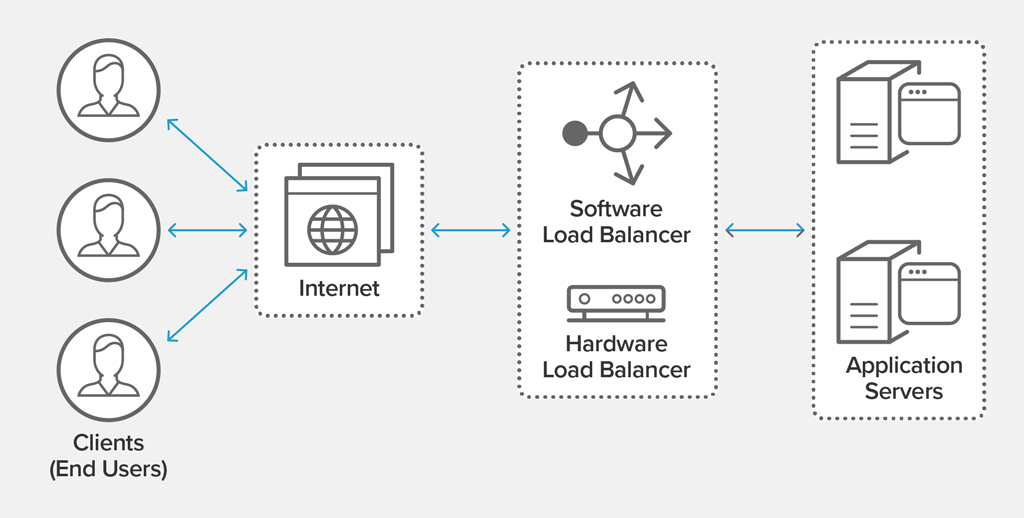
* Classic load blancer

It provides basic load blancing across multiple amazon ec2 instances and operates at both request and connection level

* Gateway load blancer

It is used for third party authorities

Architecture of load blancer:



Autoscaling:

It is service that monitors and adjust computer resources to maintain resources it allows you to automatically increase or decrease resource capacity in relation to the demand.

Types of Autoscaling:

* Vertical scaling:changing instances
* Horizontal scaling:adding no.of instances

Benefits of Autoscaling:

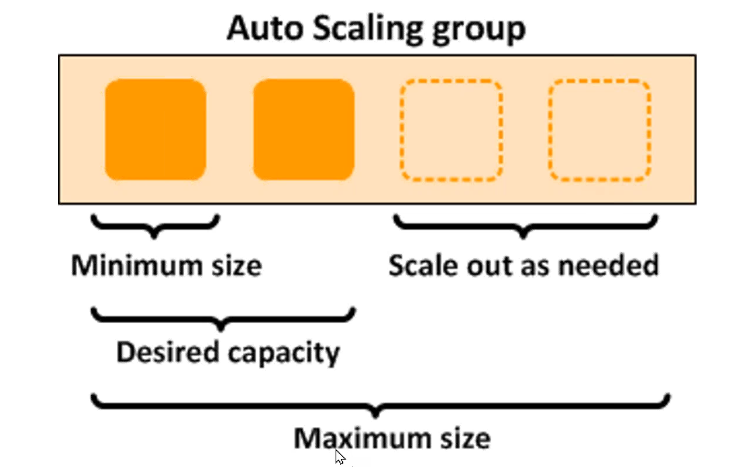
* Better Availability
* Better Fault tolerance
* Better cost managemet

Launch Configuration:

An instance configuration template that an autoscaling group uses to launch ec2 instances.when we create a launch configuration you specify information for the instance

Autoscaling group:

Contains a collection of ec2 instance that are treated as a logical grouping for the purpose of automatic scaling.



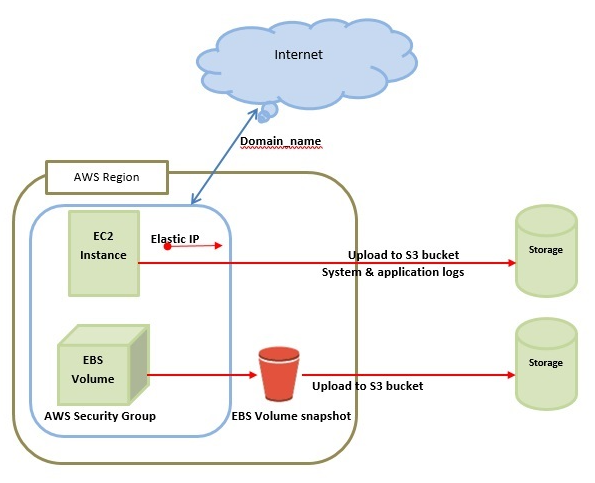
Why do we need to use EC2?

By using AWS EC2 **helps users to avoid the investment in hardware up front, so the user can deploy and develop applications easier**. It is used to launch many virtual servers, configure networking and security, and managing storage.

Where do we need to use EC2?

Amazon EC2 provides scalable computing capacity in the AWS cloud. Leveraging it enables **organizations to develop and deploy applications faster, without needing to invest in hardware upfront**. Users can launch virtual servers, configure security and networking, and manage cookies from an intuitive dashboard

Architecture diagram:



S3:Simple Storage Service

* It provides web service.it can store &retrieve the huge amount of data
* Faster performance
* It needs proper authentication
* We can access data from anywhere
* S3 stored in region not in available zone because it is globle service

Features of s3

* Lowcost: compared to all other strorage services
* Scalability: Use as much as data we want.There is no limit for data storage
* Availability: Data is always available for us
* Security: very secure,we can also encrypt the data
* Flexiblity: very flexibility we can access from anywhere

Bucket:

* Bucket is nothing but root folder in s3
* In bucket we have subfolders

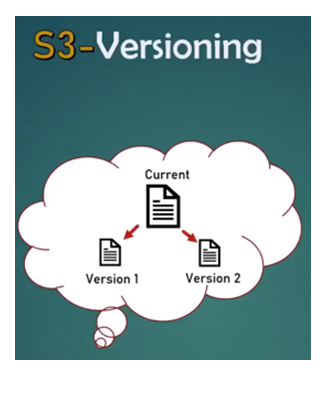
Objects:

* Object is nothing but file what we have upload in s3 bucket



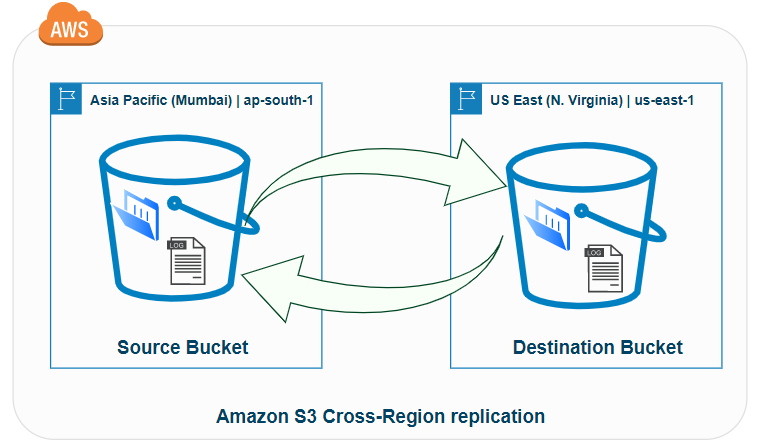
Versioning:

* It means keeping multiple varients of an object in the same bucket.It is used to preserve,retrieve and restore of every object stored in s3 bucket



Replication:

* It is feature in s3 that copies every object from source bucket to destination bucket
* That means whatever the object we uploaded in source bucket that same object will reflect to the destination bucket
* If we did’nt enable the version of both buckets replication will not work



Why do we need to use s3?

Amazon S3 is an object storage service that offersindustry-leading scalability, data availability, security, and performance. You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere.

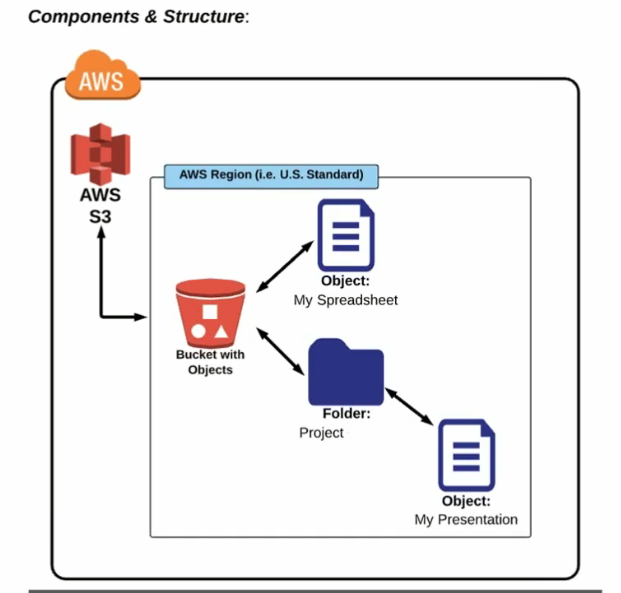
Where do we need to use s3?

An Amazon S3 bucket is a public cloud storage resource available in AWS, an object storage offering. Amazon S3 buckets, which are similar to file folders, store objects, which consist of data and its descriptive metadata.

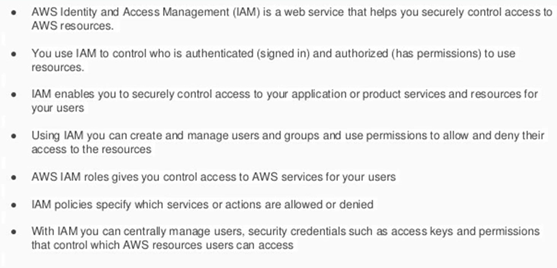
On what case we need to use?

Amazon S3 is ideal when you want to store application images and videos, and render with faster performance. All AWS services (including Amazon Prime and Amazon.com), as well as Netflix , use Amazon S3 for this purpose

Architecture diagram:



IAM: Identity and Access Management



**Features of IAM**

Following are the prominent features of IAM in AWS service.

* **Multifactor Authentication :** IAM improves the security of AWS by adding multiple authentication steps for our accounts. It is second level security
* **Cost factor :** Unlike other AWS services , IAM is free of cost . The charges are only added when we use AWS services with IAM users.
* **Shared account access :** Users can share resources with the help of AWS’s shared access features .
* **Centralized account control :** Our AWS account has centralized control so that we can create new users and groups . We can also use cancel services (or) resources using centralized control.
* **Permissions for users :** IAM has administrative rights , so uers can use it to grant access permissions.

**Components Of IAM :**

**USERS :** users are the ones with access to services on our AWS account .

**POLICIES :** Policies are the permissions to access to various AWS services .

**GROUP :** A collection of IAM users managed as a unit .

**ROLE :** IAM role defines the set of permissions for making AWS service request .

What Are The IAM Identities

There are two main types of IAM identities. They are:

* **IAM Users:**It’s a resource in IAM with credentials and permissions
* **IAM Roles:** We can create IAM roles in our account using specific permissions

IAM password policy?

Checks if the account password policy for IAM users meets the specified requirements indicated in the parameters.

* Password expiration

Password will be expired after few days

Example:Netbanking

* Prevent password reuse(imp in real time)

It doesn’t allow previous password for security purpose

Credential Report:

It is managed by architrcts and managers contains all important details

WHY SHOULD WE USE THE AWS IAM ?

* Various users can access AWS resources securely.
* Manage IAM users along with their accesses.
* Assign users individual security credentials like passwords , access keys , etc.,
* Specify permissions for users to control the operations they can access.
* Manage federated (group of organizations , regions , countries , etc.,) users in the corporate directory.
* Request security credentials for them with configurable expirations.
* Secure AWS access for employees and applications.

Where do we need to use IAM

Manage IAM users and their access – You can create users in IAM, assign them individual security credentials (in other words, access keys, passwords, and multi-factor authentication devices), or request temporary security credentials to provide users access to AWS services and resources

WHAT IS MFA:

For increased security, AWS recommends that you configure AWS Multi-Factor Authentication (MFA) to help protect your AWS resources. AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your user name and password.

## **Why AWS MFA is Required**

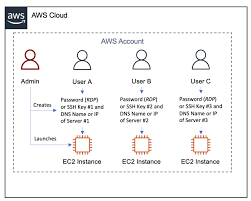
* Users have access to your account and can possibly change configurations and delete resources in your AWS account, so to overcome this it is required
* If you want to protect your root accounts and IAM user.
* Even if the password is stolen or hacked, the account is not compromised.
* When you enable this authentication for the root user, it affects only the root user credentials. IAM users in the account are distinct identities with their own credentials, and each identity has its own MFA configuration.

## What if the MFA device does not work?

If your virtual MFA device or hardware MFA device appears to be functioning properly, but you cannot use it to access your AWS resources, it might be out of synchronization with AWS. For information about synchronizing a virtual MFA device or hardware MFA device, resynchronize your virtual and hardware MFA devices.

If your AWS account root user multi-factor authentication (MFA) device is lost, damaged, or not working, you can recover access to your account. IAM users must contact an administrator to deactivate the device.

Architecture diagram:



Cloudwatch:

* It is monitoring tool
* Amazon CloudWatch allows you to collect, access, and correlate this data on a single platform from across all your AWS resources, applications, and services .

Components of cloudwatch:

1. Dashboard

2. Alarm

3. Metric

4. Aamazon Bridge Events

5. Logs

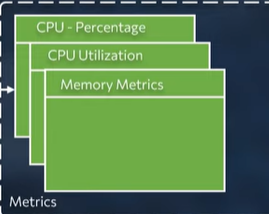
6. Rule

Dashboard:

* Dashboards are customizable homepage in cloudwatch console that we can use to monitor our resources in a single view

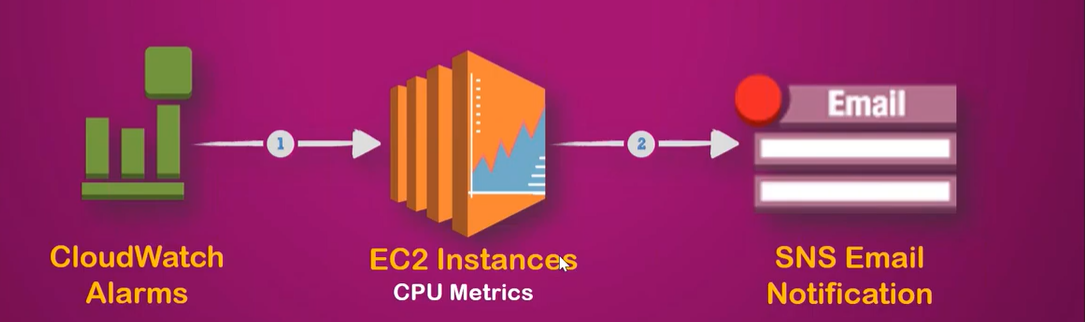
Metrics:

* It is fundamental concept. A metric represents a time-ordered set of data points that are published to Cloudwatch.
* Eg:CPU Utilization ,NetworkIn ,NetworkOut ..etc setting some metric points by using threshold level in alarm.



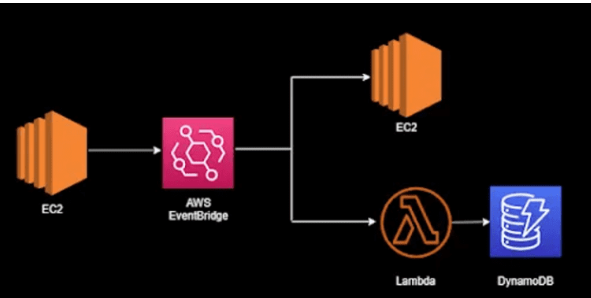
Alarms:

* It allows you to watch cloudwatch metrics and to receive notification when metrics fall outside the level that we can configure in metrics
* If the metric reached to the tigger point through mail on notification will occure and the instance will stop automatically



AmazonBridgeEvents:

* AWS CloudWatch Events enables developers to integrate many of the AWS services through events(EC2,lambda)
* By using cran we can schelude a event to stop the ec2 instance at some particular date time day..etc
* Why do we need:if we dont need of the server at that time(particular) we can use Bridge Event to implement on the server’s.



Stop instance

Termiate instance

Logs:

* Logs are used for backup purpose to a server if we required for a days backup or hours backup ‘s it will show in details .

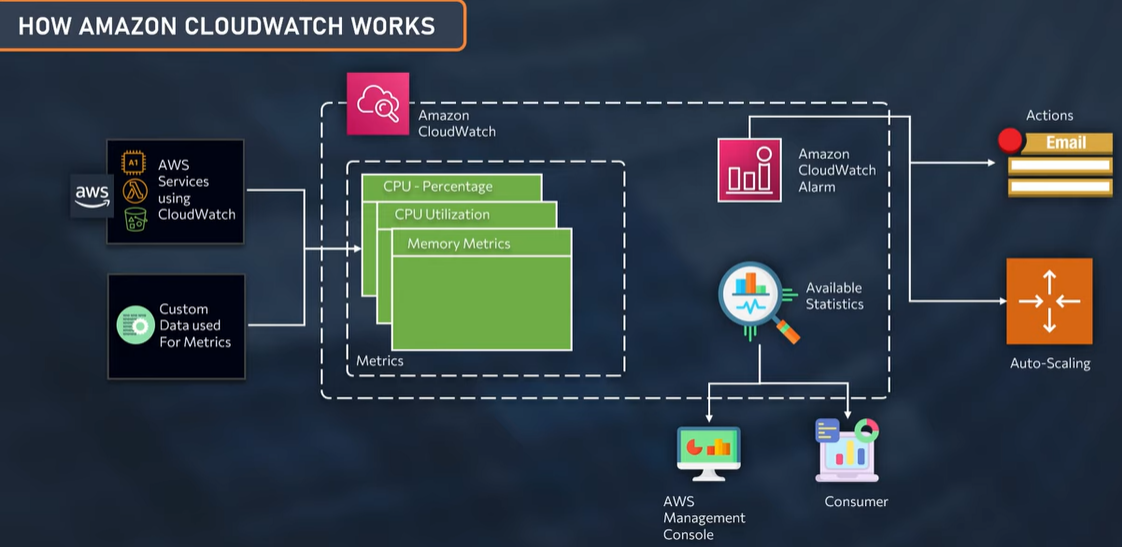
Rule:

* Defines a set of actions that are run upon the occurrence of specific event conditions

Why do we need to use cloudwatch?

CloudWatch enables you to monitor your complete stack (applications, infrastructure, and services) and use alarms, logs, and events data to take automated actions and reduce mean time to resolution (MTTR). This frees up important resources and allows you to focus on building applications and business value.

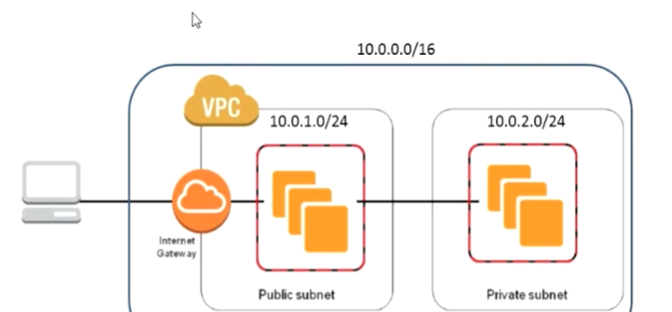
Architecture diagram:



VPC: Virtual Private Cloud

* Amazon vpc enables you to launch AWS resources into a virtual network that you have defined
* VPC is basically virtual network that we define the virtual network can have multiple subparts can have multiple configures

VPC works:



Components of VPC:

* Subnets
* RouteTables
* Internet Gateway
* Nat Gatway
* Peering Connections

Subnets:

* A subnet is a range of ip’s address in your subnet by routing traffic to virtual private gateway ,we specify’ s ipv4 &CIDR(Classless Inter Domain Routing) blocks.

CIDR: Classess Inter-Domain Routing

* This cidr block determines the range of ip address allocated for your apps in the vpc
* The size of this CIDR needs to be a number b/w 24 and 16

24 (256 ip’s)

10.0.0.0/16 to 32

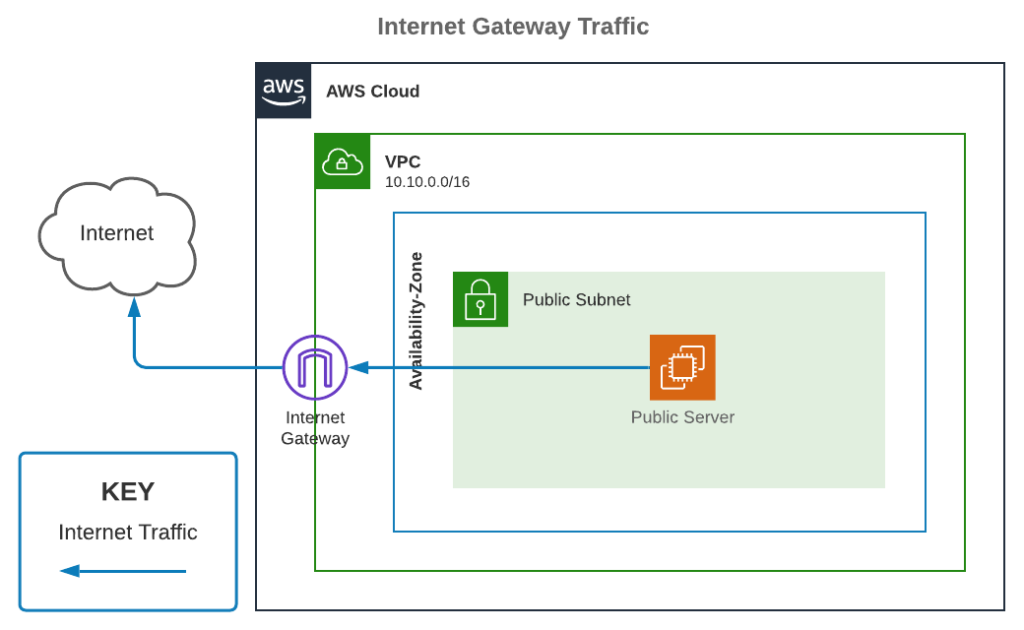
16 (65,536 ip’s)

**Route Tables:**

* A route table contains a set of rules, called routes that are used to determine where network traffic from your subnet is directed.

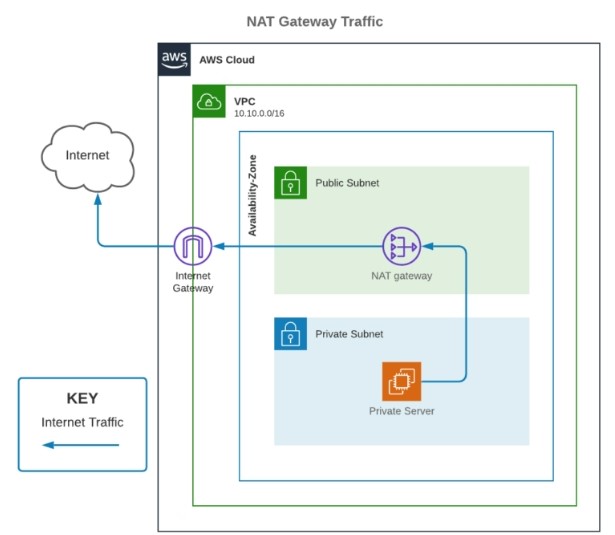
**Internet Gateway:**

* An Internet Gateway is a VPC component that allows communication between the VPC and the Internet.
* It is bidirectional communication ,by assigning internet gateway in route table then only it access to the internet.
* It provides internet access to public subnet



**Nat Gateway**:

* Specific purpose of allowing resources in private subnet to communicate to the internet.
* It provides internet access to private subnet
* **Assign a route in the private subnet of a route to an Internet Gateway , Traffic destined for the Internet will flow from the private subnet to the NAT Gateway in the public subnet, and then out to the Internet through the Internet Gateway.**

****

Peering Conections:

* A VPC Peering Connection is a network connection between two vpc’s that Enables the traffic between the Private IP’s.
* While we are doing vpc peering CIDR range must be different for two vpc otherwise it will show overlapped.
* Peering connection will work in same region,different region,different account

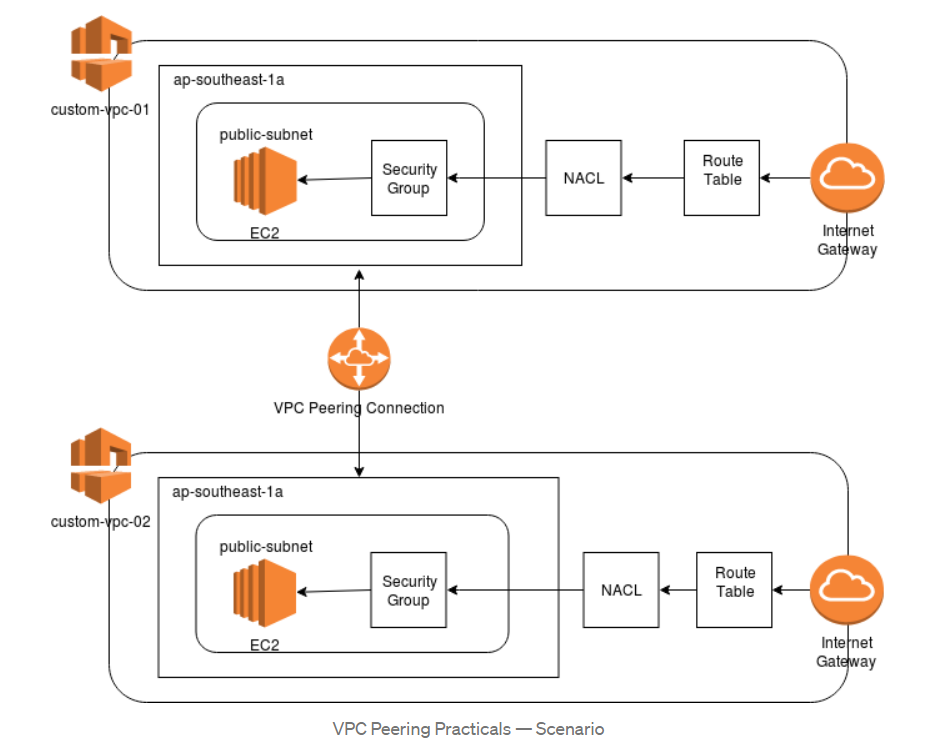
**Different types of peering connections:**

1. Same Region

2. Different Region

3. Different Account’s

Peering Architecture diagram:



**why do we need to use vpc:**

* In VPC we contain default vpc by aws server the storage of the IP address is less it will not sufficient to the servers then we go for Customiced one.
* Custom VPC‘s are easily to connect on premisses like AWS ,Azure ,Google Cloud.
* By Creating the Customiced vpc Networks we can provide how much storage required according to the servers we can assign the CIDR Blocks to the subnets
* By the formula 2 power of 32 – 2 power of n or by Subnet Calculator

**Where do we need to use VPC**:

VPCs are useful if your app needs to access servers outside of EC2, e.g. if you have a common service that's hosted in your own physical data center and not accessible via the internet. If you're going to put all of your web and DB servers on EC2, there's no reason to use VPC.

Architecture diagram:

