Introduction: -

1. What is cloud computing?

Ans: - cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics etc.

2. Deployment Model in Cloud?

Ans: - Types of Cloud Computing Deployment Models:

Public cloud:

- The Services which are associate by everyone like AWS, GCP, Azure etc.
- Public Cloud less secure as it is open to everyone.

Private Cloud:

- The services which are associate with in the organization like oracle.
- It is suitable for corporate information to which only authorized staff has access.

Hybrid Cloud:

- Hybrid cloud is combination of public and private cloud.
- Data is properly separated, So it reduce chance of data theft or allected.

Community Cloud:

- It is same as Private cloud, but can be accessible from new organization.
- It provides better security and cost effective.

Multi-Cloud:

- You can mix and match the best feature of each cloud providers services to suit the demand of your apps.

3. Service Model in Cloud?

Ans: - Infrastructure as a Service (IaaS):

- Infrastructure as a Service (IaaS) is a self-service model for managing remote data centre infrastructures. IaaS provides virtualized computing resources over the Internet hosted by a third party such as Amazon Web Services, Microsoft Azure or Google.

Platform as a Service (PaaS):

- Platform as a Service (PaaS) allows organizations to build, run and manage applications without the IT infrastructure. This makes it easier and faster to develop, test and deploy applications.

Software as a Service (SaaS):

- Software as a service (SaaS) replaces the traditional on-device software with software that is licensed on a subscription basis. It is centrally hosted in the cloud. A good example is Salesforce.com.

4. Architecture of Cloud Computing?

Ans: - The cloud architecture is divided into 2 parts:

- **Frontend –**
  Frontend of the cloud architecture refers to the client side of cloud computing system.
- **Backend –**
  Backend refers to the cloud itself it includes huge storage, virtual applications, virtual machines, traffic control mechanisms, deployment models, etc.

5. AWS Global Infrastructure Count?

Ans: - The AWS Cloud spans 105 Availability Zones within 33 geographic regions around the world, with announced plans for 12 more Availability Zones and 4 more AWS Regions in Germany, Malaysia, New Zealand, and Thailand.

6. Why do we use region?

Ans: - Regions play an important role in human geography because they show both the combinations and differentiations of culture throughout the world.

7. What is service? & What are resources?

Ans: -

- **Service: -**
  cloud provider–from infrastructure technologies like compute, storage, and databases–to emerging technologies this is called service.
- **Resource: -**
  In AWS, a resource is an entity that you can work with. Examples include an Amazon EC2 instance, an AWS CloudFormation stack, or an Amazon S3 bucket.

<u>IAM:</u> -

1. How many resources do we have in IAM?

Ans: -

- IAM Users
- IAM Groups
- IAM Roles
- Policies

2. Deployment model in IAM?

Ans: - On-Premises IAM Deployment:

- In an on-premises IAM deployment, the IAM infrastructure is installed and maintained within the organization's physical data centres.
- Organizations have direct control over the hardware, software, and network infrastructure.

Cloud-Based IAM Deployment:

- In a cloud-based IAM deployment, the IAM infrastructure is hosted and managed by a third-party cloud service provider.
- Organizations leverage IAM services provided by cloud platforms such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform.

Hybrid IAM Deployment:

- In some cases, organizations adopt a hybrid IAM deployment model, which combines elements of both on-premises and cloud-based IAM.
- This allows organizations to maintain certain IAM components on-premises while leveraging cloud-based IAM services for specific use cases or functionalities.

3. Identities in IAM?

Ans: -

- ❖ User Identities:
  User identities represent individuals within the organization. These can include employees, contractors, partners, or anyone who requires access to resources.
- ❖ Group Identities:
  Group identities allow organizations to group users based on common attributes, roles, or responsibilities. Permissions can be assigned to groups, simplifying access management.
- ❖ Service Accounts:
  Service accounts are special-purpose identities used by applications, scripts, or services to access resources. They are often used in automated processes and don't represent human users.
- ❖ Role-based Access Control (RBAC):
  RBAC is a model in which access permissions are associated with roles, and roles are assigned to identities. This helps in simplifying access management by grouping similar responsibilities and permissions together.
- ❖ Attributes and Claims:
  Identities often have associated attributes or claims that provide additional information about the user. These attributes can include things like job title, department, and other relevant information used for access decisions.

4. What is an IAM User?

Ans: - An IAM user is a resource in IAM that has associated credentials and permissions. An IAM user can represent a person or an application that uses its credentials to make AWS requests.

5. What is the IAM Group?

Ans: - An IAM group is an identity that specifies a collection of IAM users.

6. What is the IAM Policy?

Ans: - IAM policies define permissions for an action regardless of the method that you use to perform the operation.

7. What is the IAM Role?

Ans: - Roles are entities you create and assign specific permissions to that allow trusted identities such as workforce identities and applications to perform actions in AWS.

8. Where do we attach Identity Based Policy?

Ans: - Identity-based policies are attached to an IAM user, group, or role.

9. Where do we attach Resource Based Policy?

Ans: - Resource based policy means policy can attach the services resource.

10. Can we be able to create Policy via json code ?

Ans: - You can create policies in either JSON or YAML, regardless of whether you define the policy by using Monitoring filters or Monitoring Query Language (MQL).

11. What is dominator policy?

Ans: - Dominator policy means firstly read the policy that means the deny policy.

12. What is ARN? What are the fields in ARN?

Ans: - ARN typically stands for "Amazon Resource Name," and it is a term associated with Amazon Web Services (AWS).

arn:aws:service:region:account-id:resource-type/resource-id

13. How many types of ARN Partition?

Ans: - There are three primary partitions: -

- ❖ aws: - This is the default partition used for most AWS services and regions.
- ❖ aws-cn: - This partition is used for AWS China (Beijing) Region and AWS China (Ningxia) Region.
- ❖ aws-us-gov: - This partition is used for AWS GovCloud (US) regions, which are designed for U.S. government customers.

14. What are Tags?

Ans: - In the context of computing and cloud services, including Amazon Web Services (AWS), "tags" refer to metadata that you can associate with resources.

<u>S3</u>: -

1. Difference between Block storage & Object Storage?

Capability	Block storage	Object storage
Storage capacity	Limited	Nearly unlimited
Storage method	Data stored in blocks of fixed size, reassembled on demand	Unstructured data in non-hierarchical data lake
Metadata	Limited	Unlimited and customizable

Data retrieval method	Data lookup table	Customizable
Performance	Fast, especially for small files	Depends, but works well with large files
Cost	Depends on vendor, usually more expensive	Depends on vendor, usually less expensive

2. Difference between static website & dynamic website?

SL.NO	Static Web Page	Dynamic Web Page
1.	In static web pages, Pages will remain same until someone changes it manually.	In dynamic web pages, Content of pages are different for different visitors.
2.	Static Web Pages are simple in terms of complexity.	Dynamic web pages are complicated.
3.	In static web pages, Information are change rarely.	In dynamic web page, Information are change frequently.
4.	Static Web Page takes less time for loading than dynamic web page.	Dynamic web page takes more time for loading.
5.	In Static Web Pages, database is not used.	In dynamic web pages, database is used.

3. What are the naming rules?

Ans: - Between 1 and 256 characters, inclusive. Contain alphanumeric characters (A-Z, a-z, 0-9), hyphens (-), forward slashes (/), and underscores (_) Cannot begin with aws.

4. What is the major resource of S3 Bucket?

Ans: -

- Bucket Name
- Region
- Object Storage
- Access Control
- Versioning
- Logging and Monitoring
- Lifecycle management
- Encryption

5. Why do we need to host static websites instead of dynamic websites?

Ans: -

- Cost-Effectiveness
- Scalability
- Security
- Content Updates
- Reliability
- SEO (Search Engine operation)

6. What is versioning & why do we need versioning?

Ans: - Versioning is the practice of assigning unique identifiers or labels to different versions of a software application, a document, a

dataset, or any other type of information. The purpose of versioning is to keep track of changes over time, allowing users to understand, manage, and access different iterations of a particular piece of information.

- ❖ History and Auditing
- ❖ Collaboration
- ❖ Rollback and Recovery
- ❖ Testing and QA
- ❖ Release Management

7. What are the objects and types of objects that we are uploading into the S3 Bucket?

Ans: - Upload any file type-images, backups, data, movies, and so on—into an S3 bucket. The maximum size of a file that you can upload by using the Amazon S3 console is 160 GB. To upload a file larger than 160 GB.

8. Why is MFA Delete important in S3 Bucket object level?

Ans: - MFA delete can help prevent accidental bucket deletions by requiring the user who initiates the delete action to prove physical possession of an MFA device with an MFA code and adding an extra layer of friction and security to the delete action.

9. What is S3 Multipart upload?

Ans: - Amazon S3 Multipart Upload is a feature provided by Amazon Simple Storage Service (S3) that allows you to upload large objects in parts. This feature is particularly useful when dealing with files that are larger than 100 megabytes (MB) in size, as it enables more efficient and resilient uploads.

10. What are the storage classes in Amazon S3? —---------- - IMP

Ans: -

❖ S3 Standard:

- Offers high durability, availability, and performance.
- Suitable for frequently accessed data.
- It is designed to provide low-latency and high-throughput performance.

❖ S3 Intelligent-Tiering:

- Automatically moves objects between two access tiers (frequent and infrequent access) based on changing access patterns.

❖ S3 Standard-IA (Infrequent Access):

- Provides the same performance as S3 Standard but at a lower cost.
- Suitable for data that is accessed less frequently but still requires rapid access when needed.
- It has a lower storage cost compared to S3 Standard, but retrieval costs are higher.

❖ S3 One Zone-IA:

- Similar to S3 Standard-IA but stores data in a single availability zone.
- Offers lower costs compared to S3 Standard-IA but with the trade-off of reduced durability because it does not replicate data across multiple zones.

❖ S3 Glacier:

- Amazon S3 Glacier and S3 Glacier Deep Archive are archival storage classes designed for long-term data retention and cost-effective archiving.
- Retrieval times are longer compared to standard storage classes, and costs are lower.

❖ S3 Glacier Deep Archive:

- Provides the lowest storage costs among all S3 storage classes.

11. What is ACL?

Ans: - ACL stands for Access Control List. In the context of computing and information security, an Access Control List is a set of rules or permissions attached to an object that specifies which users or system processes are granted access to that object and what operations are allowed on it. ACLs are used to control access to resources and protect them from unauthorized access or modification.

12. Why do we need ACL?

Ans: - Access control lists are used for controlling permissions to a computer system or computer network. They are used to filter traffic in and out of a specific device. Those devices can be network devices that act as network gateways or endpoint devices that users access directly.

13. What is a Life cycle policy? Why do we need to use the life cycle rule?

Ans: - Life cycle policy: - Lifecycle Policy or Lifecycle Rule refers to a set of rules that define actions to be taken on objects stored in an S3 bucket over time.

The primary reason for using Lifecycle Rules is cost optimization. For example, you might initially store data in the Standard class for anything that is frequently being access.

14. How can we make our bucket public?

Ans: -

Step 1: - Create bucket and put object.

Step 2: - Inter to this bucket ACL enable and Block all public access off.

Step 3: - All object makes ACL

These steps complete then your bucket and objects are public.

15. What is CORS?

Ans: - CORS defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. This is useful because complex applications often reference third-party APIs and resources in their client-side code

16. What is S3 Inventory?

Ans: - Amazon S3 Inventory provides a flat file list of your objects and metadata, on a schedule that you define.

17. What does it mean by Requester pays?

Ans: - Requester Pays buckets, the requester instead of the bucket owner pays the cost of the request and the data download from the bucket. The bucket owner always pays the cost of storing data.

18. What is the secondary word to Transfer acceleration? Why do we need to use this transfer acceleration?

Ans: - Amazon S3 Transfer Acceleration is a bucket-level feature that enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket.

AWS Cloud Trail: -

1. What is a cloud trail?

Ans: - CloudTrail provides visibility into user activity by recording actions taken on your account.

2. Why do we use trails, what is the exact purpose of enabling the trail in cloud production accounts?

Ans: - For an ongoing record of events in your AWS account, create a trail. A trail enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions in the AWS partition in which you are working.

3. Real time use case of cloud trail?

Ans: - A company hosts critical applications and sensitive data on AWS. The security team wants to monitor all activities within their AWS environment to detect and respond to any suspicious or unauthorized actions.

4. What is cloud trail event history?

Ans: - The CloudTrail Event History is a feature within AWS CloudTrail that provides a searchable record of the past 90 days of activity in your AWS account. It allows you to view, search, and download detailed information about events and API calls made within your AWS environment.

5. What is log file integrity validation in cloud trail?

Ans: - Log File Integrity Validation is a feature provided by AWS CloudTrail that helps ensure the integrity of log files generated by CloudTrail. This feature is designed to detect and alert on any potential tampering or modification of CloudTrail log files, providing an additional layer of security and reliability for the log data.

AWS SNS: -

1. What is SNS?

Ans: - SNS stands for Simple Notification Service, and it is a fully managed messaging service provided by Amazon Web Services (AWS). SNS enables the creation and delivery of messages or notifications to a distributed set of recipients or subscribers.

2. Why do we use SNS?

Ans: - It enables you to build distributed, scalable, and highly available applications by allowing you to send messages or notifications to a distributed set of subscribers or endpoints.

3. What is an Amazon SNS function, and how we can configure it.

Ans: - Amazon Simple Notification Service (Amazon SNS) is a managed service that provides message delivery from publishers to subscribers.

4.Difference between Amazon SNS & Amazon SQS.

AMAZON SNS	AMAZON SQS
It is based on Publisher/Subscribe system	It is a Queuing service for message processing
Publishing messages can deliver to many subscribers (fan-out) of different types (SQS, Lambda, Email)	A system must poll to discover new events, and messages are typically processed to a single consumer.
All the consumers are of different types.	All the consumers are supposed to be of identical types
It involves a push mechanism with entities such as topics and broadcasts.	It involves a pull mechanism with entities such as Queue, FIFO.

5. What are the different delivery formats and transports in AWS SNS?

Ans: - The notification message sent by Amazon SNS for deliveries over
HTTP, HTTPS, Email-JSON and SQS transport protocols will consist of a simple JSON object.

6. What is 10DLC in AWS?

Ans: - Ten-Digit Long Code, or more commonly shortened as 10DLC, is intended specifically for sending Application-to-Person (A2P) SMS in the United States only.

7.What are FIFO topics on SNS?

Ans: - Amazon SNS FIFO (first in, first out) topics with Amazon SQS FIFO queues to provide strict message ordering and message deduplication.

8. What is SNS Mobile Push?

Ans: - Push notifications are messages that can be sent directly to a user's mobile device.

AWS EC2: -

1. **What is EC2, why do we need EC2 service in cloud computing?**
2. **Features of Amazon EC2?**

Ans: - Amazon Elastic Compute Cloud (Amazon EC2) is a web service provided by Amazon Web Services (AWS) that enables users to rent virtual servers, known as instances, on which they can run their applications. EC2 is a fundamental and widely-used component of AWS, offering scalable computing resources in the cloud.
Here are some key features and reasons why EC2 is essential in cloud computing:

Scalability: EC2 allows users to easily scale their computing capacity up or down based on demand. This is particularly useful for applications with varying workloads, as users can add or remove instances to match the current requirements.

Flexibility: EC2 provides a variety of instance types optimized for different use cases, such as compute-optimized, memory-optimized, storage-optimized, and GPU instances. Users can choose the instance type that best suits their application's requirements.

Cost-Efficiency: Instead of investing in physical hardware, users can pay for EC2 instances on a pay-as-you-go basis. This allows for cost savings as users only pay for the resources they consume, and they can easily adjust their capacity as needed.

Security: AWS provides various security features for EC2 instances, including network firewalls (security groups), encryption, and identity and access management (IAM) for controlling access to resources.

Reliability: EC2 instances are hosted in multiple, geographically distributed data centers, ensuring high availability and fault tolerance. Users can deploy their applications across multiple availability zones to enhance reliability.

Customization: Users have the ability to customize their virtual instances by choosing the operating system, instance type, storage, and networking configurations. This allows for tailored solutions to meet specific application requirements.

Elastic Load Balancing: EC2 instances can be used in conjunction with Elastic Load Balancing (ELB) to distribute incoming traffic across multiple instances, ensuring better availability and fault tolerance.

2. Features of Amazon EC2?

Ans: -

- Virtual Servers (Instances)
- Scalability
- Variety of Instance Types:
- Amazon Machine Images (AMIs)
- Pay-as-You-Go Pricing
- Elastic Load Balancing (ELB)
- Auto Scaling
- Security Groups and Virtual Private Cloud (VPC)
- Monitoring and Metrics:
- Integration with AWS Marketplace

3. What is Hypervisor? and its types?

Ans: - A hypervisor, also known as a Virtual Machine Monitor (VMM), is a software or hardware layer that enables multiple operating systems (OS) to run on a single physical host machine. The primary purpose of a hypervisor is to manage and allocate the host's resources, such as CPU, memory, storage, and

networking, among the virtual machines (VMs) running on it. Hypervisors play a crucial role in virtualization, allowing for the efficient and simultaneous operation of multiple independent computing environments on a single physical system.
There are two main types of hypervisors: Type 1 (bare-metal) and Type 2 (hosted).

Type 1 Hypervisor (Bare-Metal Hypervisor):

Definition: A Type 1 hypervisor runs directly on the host's hardware to control the hardware and to manage guest operating systems. It does not require a host operating system.

Advantages:
Typically offers better performance as it operates directly on the hardware.
Greater efficiency and resource utilization.
Well-suited for enterprise environments and server virtualization.

Type 2 Hypervisor (Hosted Hypervisor):

Definition: A Type 2 hypervisor runs on top of a host operating system and utilizes the host OS to manage hardware resources. It is often used for development, testing, or desktop virtualization.

Advantages:
Easier to set up and use, suitable for testing and development environments.
Can run on a wider range of hardware since it relies on the host OS.
Allows running virtual machines on a desktop or laptop.
Examples:
VMware Workstation
Oracle VirtualBox

Microsoft Hyper-V (when installed on a Windows operating system)

4. Where we use hypervisor?

Ans: - Hypervisors are used in various scenarios and industries to enable virtualization, which allows multiple operating systems to run on a single physical machine.

Server Virtualization:

Data Centers: In enterprise data centers, hypervisors are extensively used for server virtualization. They allow multiple virtual machines (VMs) to run on a single physical server, optimizing resource utilization and facilitating efficient management of computing resources.

Cloud Computing: Hypervisors play a crucial role in cloud computing platforms, enabling providers to offer virtual machines with varying resource capacities to users. Users can deploy and manage their applications in a virtualized environment on cloud infrastructure.

Desktop Virtualization:

Development and Testing: Hypervisors are used to create isolated virtual environments for development and testing purposes. Developers can test software on different operating systems and configurations without the need for separate physical hardware.

Virtual Desktop Infrastructure (VDI): Hypervisors are employed in VDI solutions to host multiple virtual desktops on a single physical server. This allows centralized management of desktop environments and provides flexibility for end-users to access their desktops from various devices.

Education and Training:

Learning Environments: Educational institutions use hypervisors to create virtual labs where students can practice and experiment with different operating systems and applications without the need for dedicated physical hardware.

Disaster Recovery:

Business Continuity: Hypervisors are employed in disaster recovery scenarios, where virtualization facilitates the creation of backup VMs that can be quickly activated in the event of a system failure. This helps ensure business continuity and minimizes downtime.

Consolidation and Resource Optimization:

Resource Pooling: Hypervisors enable the consolidation of multiple workloads onto a smaller number of physical servers. This helps organizations optimize resource usage, reduce hardware costs, and simplify infrastructure management.

Embedded Systems and IoT:

Testing Environments: Hypervisors are used in embedded systems development and testing to simulate different hardware configurations and test software in diverse environments.

Security and Isolation:

Security Testing: Hypervisors are used for security testing and research, creating isolated environments for analyzing malware, studying vulnerabilities, and conducting penetration testing.

Legacy Application Support:

Legacy Software: Hypervisors can be used to run legacy applications that may require older operating systems or specific hardware configurations. This allows organizations to maintain and support legacy software in a virtualized environment.

5. **EC2 Instance state and State code ?**

Ans: - Amazon EC2 instances have several instance-state codes that represent the current state of an instance. These codes help users and automated systems understand the status of an instance at any given time. As of my last knowledge update in January 2022, the following are some common EC2 instance-state codes:

0 (pending):

The instance is in the process of being launched.

16 (running):

The instance is running and has passed the initialization checks.

32 (shutting-down):

The instance is in the process of being terminated. It has received the termination signal, and the underlying resources are being released.

48 (terminated):

The instance has been permanently deleted. This is the final state after the termination process is complete.

64 (stopping):

The instance is in the process of being stopped. It has received the stop signal, and the operating system is shutting down.

80 (stopped):

The instance is fully stopped. The underlying resources are still allocated, but the instance is not actively running.

7. What is the meaning of server hibernating mode?

   Ans: - Hibernate is a feature available for certain instance types in Amazon EC2. When you hibernate an instance, the contents of the instance's RAM are preserved to its root EBS volume, and the instance enters a stopped state. When you restart the instance, it can quickly resume from its previous state, including the contents of RAM. This is particularly useful for instances with long-running applications or workloads that need to be preserved across instance stop-start cycles.

8. What is KMS?

   Ans: - KMS stands for Key Management Service. In the context of cloud computing and AWS (Amazon Web Services), AWS Key Management Service (AWS KMS) is a fully managed service that makes it easy to create and control cryptographic keys used to encrypt data. It provides a secure and scalable solution for managing encryption keys that are used to secure sensitive information across various AWS services and in your applications.

   AWS KMS allows you to create, import, and manage cryptographic keys for use with AWS services and your applications. Keys can be created through the AWS Management Console, the AWS CLI (Command Line Interface), or the AWS SDKs (Software Development Kits).

9. AWS Amazon EC2 Instance types?

Ans: - AWS Amazon EC2 Instance types ?

Amazon EC2 provides a variety of instance types, each optimized for different use cases and workloads. Instance types are categorized based on factors such as compute capacity, memory, storage, and networking capabilities. It's important to note that AWS may introduce new instance types or make updates to existing ones over time. Here are some of the common EC2 instance families as of my last update:

General Purpose Instances:

Examples:

t4g, t3, t3a, t2, t3 instances offer a balance of compute, memory, and networking resources. They are suitable for a variety of diverse workloads.

Compute Optimized Instances:

Examples:

c7g, c6g, c5, c5a, c4 instances are designed for compute-intensive applications that require high-performance processors.

Memory Optimized Instances:

Examples:

r7, r6g, r5, r5a, r4 instances are optimized for memory-intensive workloads, such as large-scale in-memory databases and real-time big data analytics.

Storage Optimized Instances:

Examples:

i3, i3en, d2 instances provide high-performance storage, making them suitable for I/O-intensive applications and large-scale data processing.

Accelerated Computing Instances:

Examples:

p4, p3, p2, inf1 instances feature GPUs or specialized hardware accelerators, making them ideal for tasks such as machine learning, graphics rendering, and video processing.

Bare Metal Instances:

Examples:

m6i, m5zn instances provide access to the underlying hardware with no virtualization overhead. They are suitable for workloads that require direct access to physical resources.

Burstable Performance Instances:

Examples:

t4g, t3, t3a instances are designed for workloads with variable performance requirements. They accumulate CPU credits during periods of low usage and use them during bursts of high activity.

Ans: - There are three type of status check

- **0/2 → AWS side Hardware Problem**
- **1/2 → Server-side software problem**
- **2/2 → All clear**

11. When we see the global view option in ec2 service?

Ans: - It shows the Summary of your resources across all Regions for which your account is enabled.

12. When we logged into the cloud account by default why do we always jump into the north Virginia region, why it's most popular?

Ans: - Since its launch in 2006, Amazon Web Services (AWS) has been constructing and operating data centres in Virginia. The facilities are a key part of the infrastructure needed to provide cloud computing power to customers.

13. What are EBS Volumes and its types?

Ans: - Amazon Elastic Block Store (EBS) provides block-level storage volumes for use with Amazon EC2 instances. EBS volumes are essentially virtual hard drives that can be attached to EC2 instances to provide scalable and persistent block-level storage.

- General Purpose (SSD) Volumes (gp2):
- Provisioned IOPS (SSD) Volumes (io2 and io1):
- Throughput Optimized (HDD) Volumes (st1):
- Cold HDD Volumes (sc1):
- Magnetic Volumes (standard):

14. Purpose of Using EBS volumes?

Ans: - EBS Volumes can be used as your primary storage device for an EC2 instance or database, or for throughput-intensive systems requiring constant disk scans. EBS volumes exist independently from your EC2 instances and can be retained after the associated EC2 instance has been deleted.

15. How many types of purchasing options do we have in aws ec2?

Ans: -

System Status Checks:

Description: System status checks monitor the health of the underlying host computer (hardware) that is running your EC2 instance. These checks are performed by the hypervisor and are independent of the operating system of your instance.

Examples of Checks:

Loss of network connectivity to the instance

Loss of system power

Software issues on the physical host

Status Results:

"ok" if the check passes

"impaired" or "initializing" if the check fails

Instance Status Checks:

Description: Instance status checks monitor the health of the instance itself, including the operating system and any applications or services running on it. These checks are performed by the instance's operating system and AWS agent.

Examples of Checks:

Failed system status checks

Incorrect networking or startup configuration

Exhausted memory or disk space on the instance

Status Results:

"ok" if the check passes

"impaired" or "initializing" if the check fails

When we see the global view option in ec2 service ?

there is no specific "global view" option in the Amazon EC2 service. The EC2 service primarily operates within specific AWS regions, and users typically interact with and manage their EC2 instances within a chosen region.

However, there are a few AWS services and features that provide a global view or operate across multiple regions:

AWS Global Accelerator:

AWS Global Accelerator is a service that provides static IP addresses and distributes traffic across multiple AWS regions. It allows you to create a single entry point for your applications, improving availability and fault tolerance.

Amazon EC2 Auto Scaling (Cross-Region):

While EC2 instances are region-specific, Amazon EC2 Auto Scaling allows you to configure auto scaling groups that span multiple regions. This enables you to automatically adjust the number of instances based on demand in different regions.

Amazon EC2 Image Builder:

Amazon EC2 Image Builder is a regional service for creating and managing Amazon Machine Images (AMIs). Although it operates within a region, you can share custom AMIs across regions.

15. What is elastic IP? & WHY were we used?

Ans: - An Elastic IP address is a static IPv4 address designed for dynamic cloud computing. An Elastic IP address is allocated to your AWS account and is yours until you release it. By using 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.

16. What is the snapshot of why we use it?

Ans: - A snapshot takes a copy of the EBS volume. The initial snapshot is a full copy of the volume; ongoing snapshots store incremental block-level changes only. It is use for Backup of our instance volume.

17. How can we save money in snapshot costing, if an automated snapshot has been created?

Ans: - Amazon EBS snapshots in AWS are an essential part of data backup and disaster recovery strategies. While the costs associated with snapshots are generally low, there are ways to optimize and save money. Here are some strategies to manage and reduce snapshot costs:

Delete Unnecessary Snapshots:

Action: Regularly review and delete snapshots that are no longer needed. This can include outdated snapshots, snapshots for volumes that are no longer in use, or snapshots that were created for temporary purposes.

Consideration: Deleting unnecessary snapshots reduces storage costs and can lead to cost savings.

Lifecycle Management:

Action: Implement lifecycle management policies to automate the deletion of snapshots based on predefined rules. AWS provides tools like AWS Backup and Amazon Data Lifecycle Manager for managing snapshots and automating lifecycle policies.

Consideration: Automating the snapshot lifecycle ensures that you adhere to your backup retention policies and helps avoid unnecessary storage costs.

Use Incremental Backups:

Action: Leverage the incremental nature of EBS snapshots. Since snapshots capture only the changed blocks since the last

snapshot, subsequent snapshots are smaller and more cost-effective.

Consideration: By using incremental backups, you minimize the amount of data stored in each snapshot, resulting in lower storage costs.

Share Snapshots:

Action: Share snapshots across AWS accounts if applicable. By sharing snapshots, you can avoid duplicating snapshots for the same data across multiple accounts.

Consideration: This is particularly useful in scenarios where multiple AWS accounts need access to the same data without incurring additional snapshot storage costs.

Use EBS Volume-Backed AMIs:

Action: When creating Amazon Machine Images (AMIs), use EBS volume-backed AMIs instead of instance-store-backed AMIs. EBS volume-backed AMIs reference snapshots, and you can manage the snapshots independently.

Consideration: This approach allows for more efficient snapshot management and control over associated costs.

Snapshot Copy Across Regions:

Action: If you need to copy snapshots to another AWS region, carefully consider the cost implications. Data transfer costs and snapshot storage costs in the destination region should be taken into account.

Consideration: Minimize cross-region snapshot copies unless necessary, as data transfer costs can contribute to the overall expense.

Use Amazon S3 Lifecycle Policies:

Action: Amazon S3 is used as the backend for storing EBS snapshots. You can set up S3 lifecycle policies to transition

snapshots to cheaper storage classes, such as Amazon S3 Glacier, after a certain period.

Consideration: This strategy helps reduce snapshot storage costs for data that is not frequently accessed.

18. Difference between Security Group & NACL?

SR NO.	Security Group	NACL
1.	Associate with EC2 Instance.	Associate with Subnet.
2.	Control traffic inbound and outbound Instance level.	Control traffic inbound and outbound subnet level.
3.	Support allow rule only.	Support allow and deny rule.
4.	Evaluate all rules before deciding whether to allow traffic.	Evaluate rule in number order when deciding whether to allow traffic. Start lowest number rule,

19. What are NACL & Its types?

Ans: - NACL: Network Access Control List, which helps provide a layer of security to the Amazon Web Services.

There are two types of NaCl:

1. **Customized NACL:** It can also be understood as a user-defined NACL, and its inherent characteristic is to deny any incoming and outgoing traffic until a rule is added to handle the traffic.

2. **Default NACL:** This is the opposite of customized NACL, which allows all the traffic to flow in and out of the network. It also comes with a specific rule which is associated with a rule number, and it can't be modified or deleted.

20. How many IP Addresses can we attach to the instances?

Ans: - In Amazon Web Services (AWS), a Virtual Private Cloud (VPC) can have a maximum of 5 IP addresses per Elastic Network Interface (ENI) and a maximum of 8,000 IP addresses per VPC.

21. What is a key pair, and its types?

Ans: - A key pair, consisting of a public key and a private key, is a set of security credentials that you use to prove your identity when connecting to an Amazon EC2 instance. Amazon EC2 stores the public key on your instance, and you store the private key.

There are two type key pair:

A key pair is a combination of a public key that is used to encrypt data and a private key that is used to decrypt data.

22. What is load balancer and its types?

Ans: - A load balancer serves as the single point of contact for clients. The load balancer distributes incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones. This increases the availability of your application.

There are four type of load balance:

- Classic load balance
- Application load balance
- Network load balance

- Gateway load balance

23. How does the load balancer work in the backend? Can you explain it?

Ans: - Load balancers increase the fault tolerance of your systems by automatically detecting server problems and redirecting client traffic to available servers. You can use load balancing to make these tasks easier: Run application server maintenance or upgrades without application downtime.

24. Features of Load Balancers?

Ans: -

❖ Distribution of Incoming Traffic:
Load balancers distribute incoming application traffic across multiple targets (e.g., EC2 instances)

❖ High Availability:
Load balancers enhance the availability of applications by spreading the traffic across multiple servers. In case one server fails or becomes unhealthy, the load balancer redirects traffic to healthy servers, providing a level of fault tolerance.

❖ Health Checks:
Load balancers regularly perform health checks on the registered targets to assess their availability. Unhealthy targets are automatically removed from the load balancing rotation until they recover.

❖ Path-Based Routing (for ALB):
Application Load Balancers (ALBs) support path-based routing, allowing you to route traffic to different backend services based on the content of the URL path.

❖ Access Logs and Monitoring:
Load balancers typically provide access logs and metrics that help monitor performance, track requests, and troubleshoot issues.

25. What is ASG? & Its types?

Ans: - An Auto Scaling group contains a collection of EC2 instances that are treated as a logical grouping for the purposes of automatic scaling and management.

- ❖ Reactive Scaling. In Reactive auto-scaling, the resources are scaled in response to traffic surges.
- ❖ Predictive Scaling. Predictive auto-scaling uses machine learning to forecast the traffic.
- ❖ Scheduled Scaling. Scheduled scaling adjusts resources based on a schedule.
- ❖ Manual Scaling.
- ❖ Dynamic Scaling.

26. What is a Health Check?

Ans: - Health checks are a way of asking a service on a particular server whether or not it is capable of performing work successfully. Load balancers ask each server this question periodically to determine which servers it is safe to direct traffic to.

27. What is the threshold?

Ans: - The memory utilization threshold, as a percent of the available memory. A value of -1 disables the threshold. The amount of time, in minutes, that the load must exceed a threshold before more instances are added or removed.

28. What is the group of LB?

Ans: - The security group for your Application Load Balancer controls the traffic that is allowed to reach and leave the load balancer.

29. Why do we prefer LB over ALB?

Ans: - An ALB is a good choice when you need flexible application-level traffic management and routing.

30. Difference between Web server & Application server?

Feature	Web Server	Application Server
Content	Intended to be used for static content	Used for dynamic content
Resources	Utilizes fewer resources than an application server	Requires more resources than a web server
Protocols	HTTP and HTTPS protocols	HTTP/S, in addition to RPC/RMI/Remoting, messaging, and other proprietary wireline protocols
Requests	Responds to HTTP requests with requested content	Dynamically generates a response for the requested resource

31. What is the target group?

Ans: - Target groups route requests to individual registered targets, such as EC2 instances, using the protocol and port number that you specify. You can register a target with multiple target groups.

32. What is the desired capacity in ASG?

Ans: - The desired capacity is the initial capacity of the Auto Scaling group.

33. Difference between vertical scaling and horizontal scaling?

Vertical Scaling	**Horizontal Scaling**
Work in backend, Developer increases the server size.	If system is crash condition, then create a multiple replica in production server.
Developer is used by testing purpose.	Costumer or end user used the server.
Additional setup in normally needed.	Resource replication and automated scaling.
Limited by maximum hardware capacity.	Not limited by hardware capacity.

34. What is difference between EBS/EFS/S3

S3	EBS	EFS

It is object storage.	It is block storage.	It is file storage.
It is unlimited storage.	It is limited storage.	It is unlimited storage.
Publicly and privately accessible.	Accessible only via the attached EC2 instance.	Accessible simultaneously from multiple EC2 and on-premises instance.
It is web interface.	It is file system interface.	It is web and file system interface.
Pay as you use.	Pay for provisioned capacity.	Pay as you use.

Virtual Private Cloud (VPC)

- **What is VPC?**

Ans: - Amazon Virtual Private Cloud (Amazon VPC), you can launch AWS resources in a logically isolated virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data centre.

- **Isolated network AWS**
- **Region specific service**
- **VPC is like our network**
- **Subnet is -AZ network**
- **We can create a multiple subnet in one AZ & multiple AZ also**
- **AWS has reserve own five (5) Ip addresses**

a) 10.0.0.0 ------ Network
b) 10.0.0.1 ------ Reserved by AWS for routers/routing purpose
c) 10.0.0.2 ------ DNS (Domain name service)
d) 10.0.0.3 ------ AWS Ip for the future use
e) 10.0.0.255 ----- Broadcast Ip

- **What is subnet?**

Ans: - A subnet is a range of Ip addresses in your VPC. A subnet must reside in a single availability zone.

- **What is Route Table?**

Ans: - To determine where network traffic from your subnet or gateway is directed.

- **What is Gateway?**

Ans: - A gateway connect your VPC to another network. Use an internet gateway to connect your VPC to the internet. Without the use of VPC an internet gateway or NAT device.

- **What is Security Group?**

Ans: - A Security Group control all traffic to the resource. You associate a security group with EC2 instance. It controls inbound and outbound traffic for the instance.

- **What is Network Access Control list (NACL)?**

Ans: - A NACL are allow and denies specific inbound and outbound traffic at the subnet level. It is additional layer of security to your VPC.

- **Type of VPC?**
  1. Default VPC always created
  2. Customer can create own VPC
  3. VPC → Subnet, CIDR, RT, DHCP
- **Range of classless Inter-Domain Routing (CIDR) in AWS?**

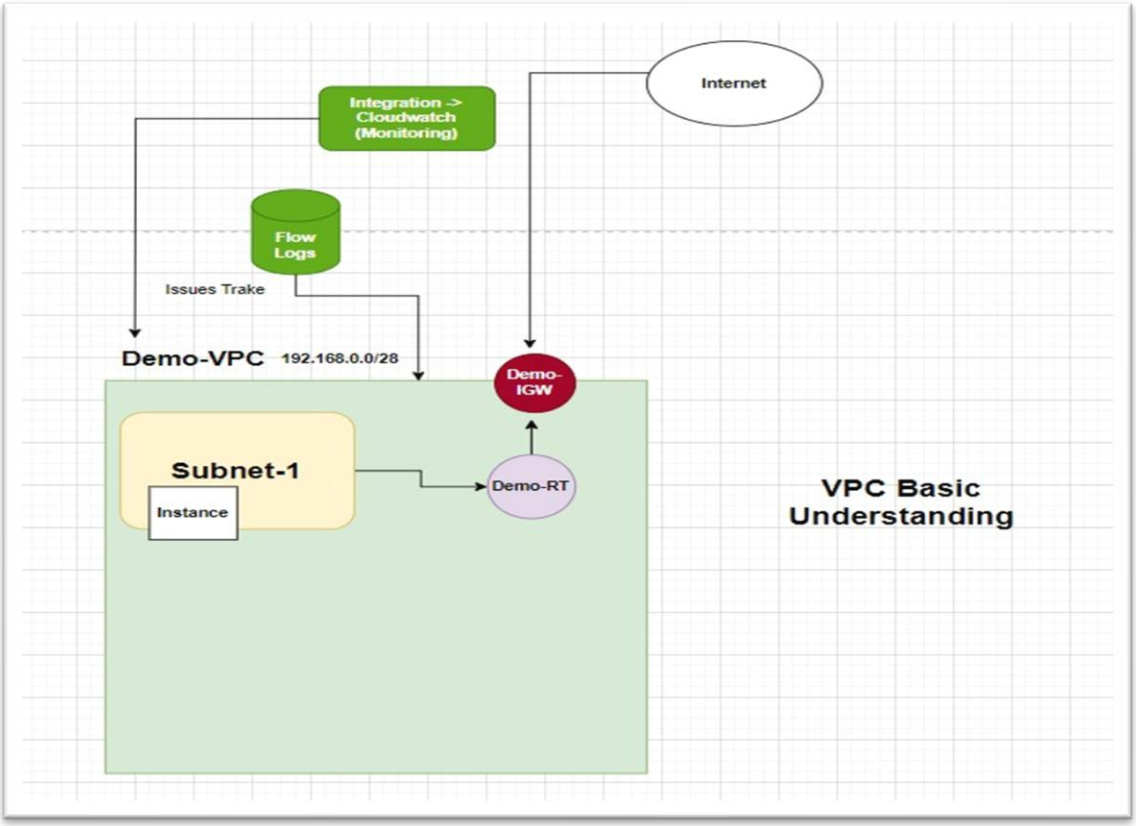
Used by AWS /16 ---------- /28 less usable host.

- **Range of Private Ip: -**
    1. Class A → 10.0.0.0 - 10.255.255.255
    2. Class B → 172.16.0.0 – 172.16.255.255
    3. Class C → 192.168.0.0 – 172.168.255.255

- **Difference between Security Group and NACL?**

Security Group	NACL
Associate with EC2 instance.	Associate with Subnet
Control traffic Inbound and Outbound Instance level.	Control traffic Inbound and Outbound subnet level.
Support allow rule only.	Support allow and deny rule.
Evaluate all rules before deciding whether to allow traffic.	Evaluate rule in number order when deciding whether to allow traffic, Starts lowest number rule.

- **Create a VPC Network.**



Step 1: - Create a VPC

VPC → Create VPC → VPC only → name → Ipv4 CIDR manual input → 192.168.0.0/26 → Create VPC

(VPC only – create manually, VPC& more – AWS create automatically VPC)

Step 2: - Create Subnet

VPC → Subnet → Create → Select VPC Id → name → Availability zone select → CIDR Block (192.168.0.0/28) → Save

Step 3: - Create gateway and attach to VPC

VPC → Internet gateway → create → name → save

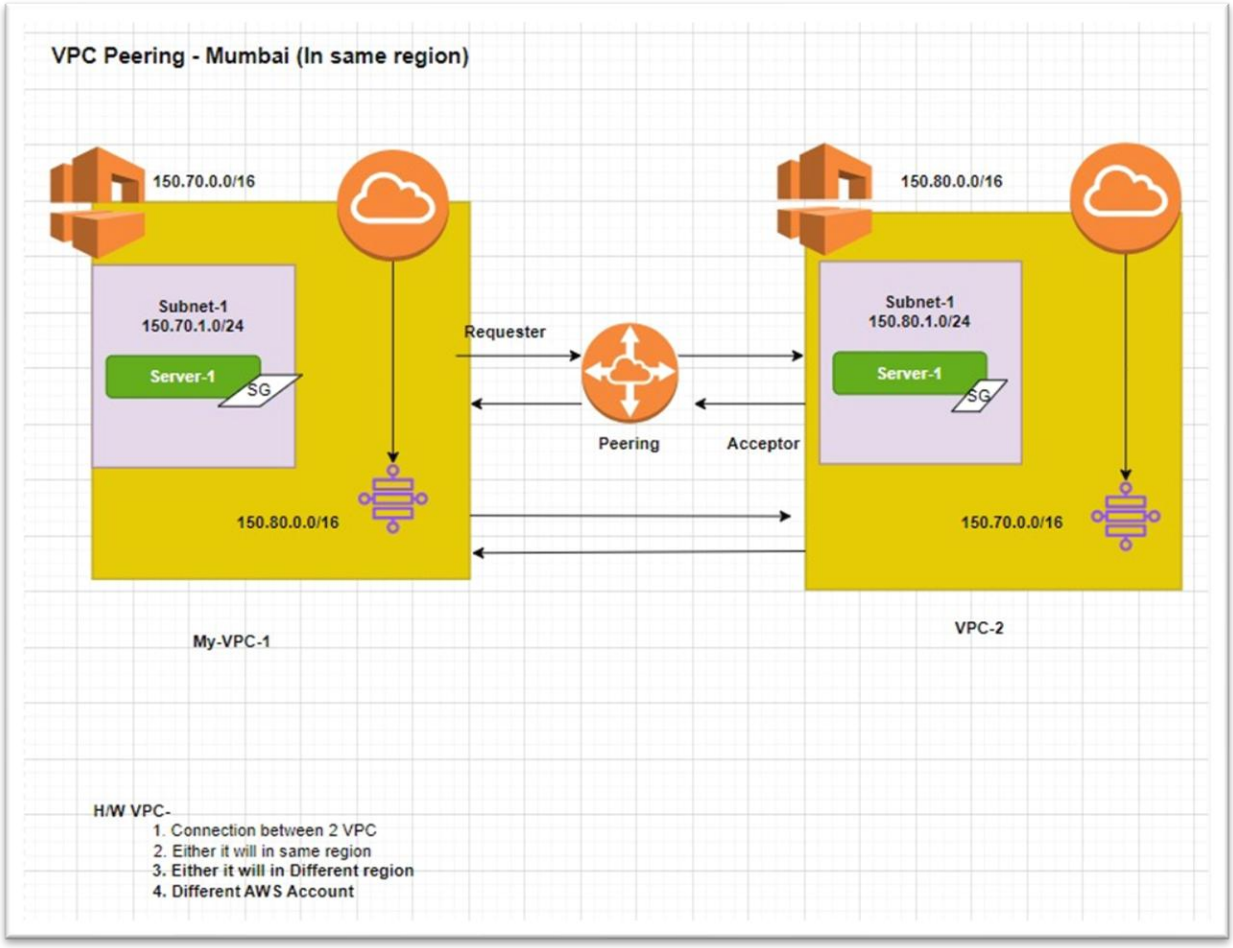
Select VPC → Action → Attach to VPC → Select VPC → Attach

Step 4: - Attach route table to gateway

VPC → Route table → select table → Action → Edit route → Add route → (Destination – 0.0.0.0/0, Target – Internet gateway) → select gateway → save

Step 5: - Create Instance and take SSH to cli and check Network proper work or not. (Security group → All ICMP-Ipv4 → 0.0.0.0/0 → save)

➢ **<u>VPC Peering Connection</u>**: -



A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. 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, or with a VPC in another AWS account. The VPCs can be in different Regions (also known as an inter-Region VPC peering connection).

Step 1: - Create a VPC-1 (Mumbai Region)

VPC → Create VPC → VPC only → name → Ipv4 CIDR manual input → 192.168.0.0/26 → Create VPC

Step 2: - Create Subnet

VPC → Subnet → Create → Select VPC Id → name → Availability zone select → CIDR Block (192.168.0.0/28) → Save

Step 3: - Create gateway and attach to VPC

VPC → Internet gateway → create → name → save

Select VPC → Action → Attach to VPC → Select VPC → Attach

Step 4: - Attach route table to gateway

VPC → Route table → select table → Action → Edit route → Add route → (Destination – 0.0.0.0/0, Target – Internet gateway) → select gateway → save

Step 5: - Create Instance (Server-1)

Step 6: - Create a VPC-2 (Tokyo Region)

VPC → Create VPC → VPC only → name → Ipv4 CIDR manual input → 172.16.0.0/16→ Create VPC

Step 7: - Create Subnet

VPC → Subnet → Create → Select VPC Id → name → Availability zone select → CIDR Block (172.16.0.0/28) → Save

Step 8: - Create gateway and attach to VPC

VPC → Internet gateway → create → name → save

Select VPC → Action → Attach to VPC → Select VPC → Attach

Step 9: - Attach route table to gateway

VPC → Route table → select table → Action → Edit route → Add route → (Destination – 0.0.0.0/0, Target – Internet gateway) → select gateway → save

Step 10: - Create instance (Server-2)

Step 11: - Create VPC Peering Connection

VPC → Peering Connection → Name → Select Requester VPC (VPC-1) →Select Account (My Account) → Select Region (Another Region) → Select Acceptor VPC (VPC-2) → Save

Step 12: - Modify Route Table From VPC-1 & VPC-2

VPC-1 → Route Table → Edit Route → Type VPC-2 CIDR →Select Peering Connection → Save

VPC-2 → Route Table → Edit Route → Type VPC-1 CIDR →Select Peering Connection → Save

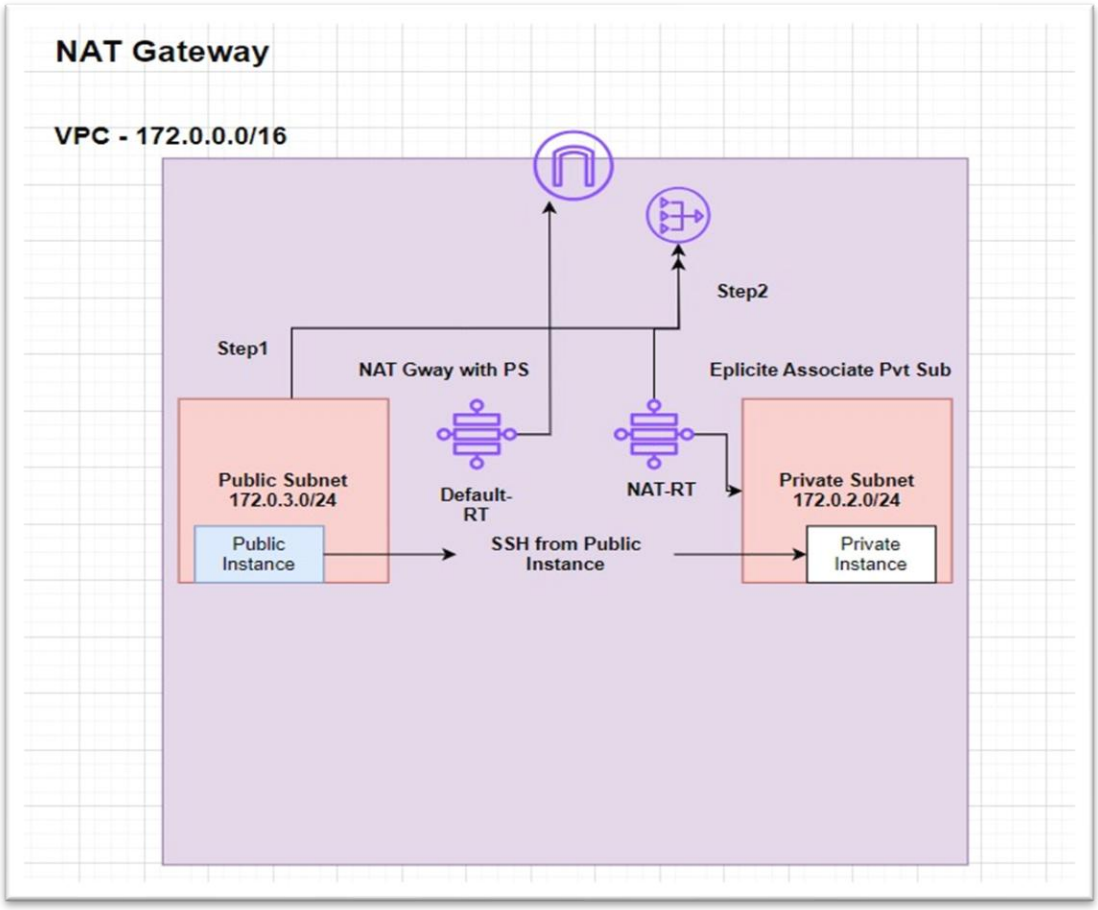
Step 13: - Add Inbound Rule in Security Group to Instances.

Server -1 →SG →Edit Inbound Rule → Custom ICMP Ipv4 →Type VPC -2 CIDR → Save

Server -2 →SG →Edit Inbound Rule → Custom ICMP Ipv4 →Type VPC -1 CIDR → Save

Step 14: - Take a SSH and ping the Server's Private Ip.

- **NAT Gateway (Bastion Host)**: -



- A NAT gateway is a Network Address Translation (NAT) service. You can use a NAT gateway so that instances in a private subnet can connect to services outside your VPC but external services cannot initiate a connection with those instances.
- NAT Gateway use to provide the internet to private server.

Step 1: - Create VPC

Step 2: - Create 2 Subnet (1 Public, 1 Private)

Step 3: - Create gateway and attach to VPC

Step 4: - Attach default route table to gateway

Step 5: - Create 2 Instances (1 Public, 1 Private)

NOTE: - If Instances Create then go through Security Group and Add →All ICMP Ipv4 → 0.0.0.0/0 →Save

Step 6: - Create Route Table (Ex: - RT -2)

Step 7: - Copy 'pem' Key data and take a SSH to Public Server and Create a new 'pem' file and paste the data and take a SSH to Private Server. (Jump public server To Private Server)

Step 8: - Create NAT Gateway use to Public Subnet

VPC → NAT Gateway → Name →Select Public Subnet → Select Connectivity Type Public → Elastic Ip Allocate → Create

Step 9: - Private Subnet Associate with the Route Table (RT -2)

VPC → RT -2 → Subnet Associate → Edit → Select Private Subnet → Save

Step 10: - NAT Gateway Attach to the Route table (RT -2)

VPC → Route Table → Edit Route → Add → 0.0.0.0/0 →Select NAT gateway → Save

Step 11: - Check the Internet ping

- **<u>VPC Endpoint</u>**: -

1. VPC Endpoint saves our costing factor, because NAT will charge by their usage and allocated elastic IP address.
2. VPC Endpoint enables you to privately access AWS services from your own VPC without using public Ip without Ip address.
3. Basically, VPC Endpoint cover two types.

a. Gateway (Accessing AWS resource internally via Routing through RT)

b. Interface (Accessing AWS resource internally via Interface)

- **Why we need to use VPC Endpoint: -**

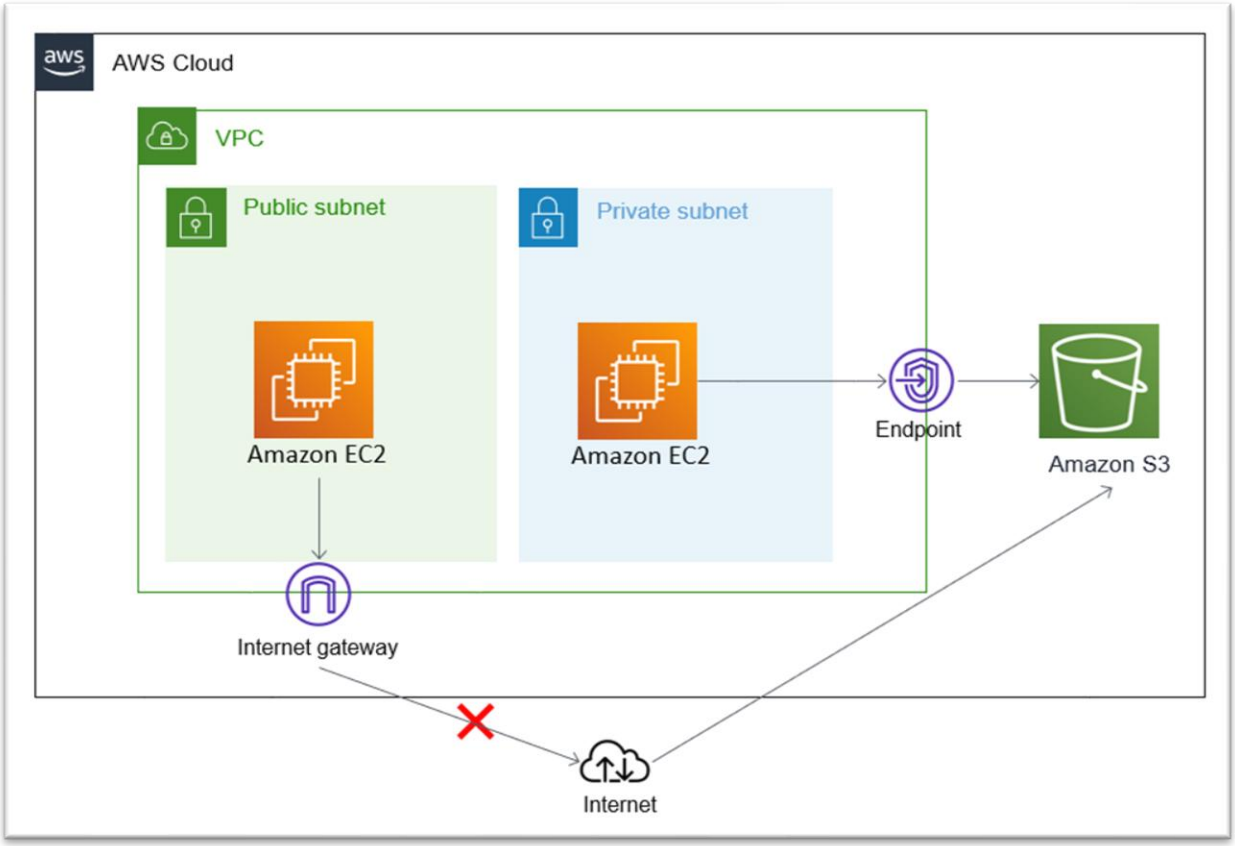
1. VPC Endpoint enables you to create private connection in between our VPC.

2. Another thing is our multiple services can communicate with each other without internet, or w/o NAT.

3. Costing factors will also come.

➢ Limitation of VPC Endpoints: -

1. VPC Endpoint and services must be in a same region.
2. VPC Endpoint supports IPv4 traffic only.
3. Endpoint is not transferable from one VPC to another different VPC.



Step 1: - Create VPC
Step 2: - Create 2 Subnet (1 Public, 1 Private)
Step 3: - Create gateway and attach to VPC
Step 4: - Attach default route table to gateway
Step 5: - Create 2 Instances (1 Public, 1 Private)

NOTE: - If Instances Create then go through Security Group and Add →All ICMP Ipv4 → 0.0.0.0/0 →Save

Step 6: - Create Route Table (Ex: - RT -2)

Step 7: - Copy 'pem' Key data and take a SSH to Public Server and Create a new 'pem' file and paste the data and take a SSH to Private Server. (Jump public server To Private Server)

Step 8: - Create NAT Gateway use to Public Subnet

VPC → NAT Gateway → Name →Select Public Subnet → Select Connectivity Type Public → Elastic Ip Allocate → Create

Step 9: - Private Subnet Associate with the Route Table (RT -2)

VPC → RT -2 → Subnet Associate → Edit → Select Private Subnet → Save

Step 10: - NAT Gateway Attach to the Route table (RT -2)

VPC → Route Table → Edit Route → Add → 0.0.0.0/0 →Select NAT gateway → Save

Step 11: - Download AWS Cli Package and Configure

- curl -O AWS URL
- Sudo apt install unzip
- Unzip aws Package
- Sudo ./aws/install

Step 12: - Delete NAT Gateway and Route Table (RT -2)

Step 13: - Create Role use of EC2 and access the S3 Bucket in Cli

Iam → Role → Create → Select AWS Service → Select use case 'EC2' → next → Select Permission Policy 'S3 Full access' → Role name → Create

Step 14: - Attach Iam Role to Private Server

EC2 → Select Private Server → Action → Security → Modify Iam Role →Select Role → save

Step 15: - Create Endpoint in S3 Gateway

VPC → Endpoint → Create → Name → Select AWS Service → Select S3 Service Gateway → Select VPC → Select Route Table 'Default' → Create

Step 16: - Check to Cli S3 Bucket (aws S3 ls)

- **Create a S3 Bucket in AWS Cli Command.**
  - aws S3 mb S3://Bucket-name --------(Create Default Region)
  - aws S3 mb S3://Bucket-name --region ap-south-1 ----(Create Selected Region)

- **Delete a S3 Bucket in AWS Cli Command.**
  - aws S3 rb S3://Bucket-name

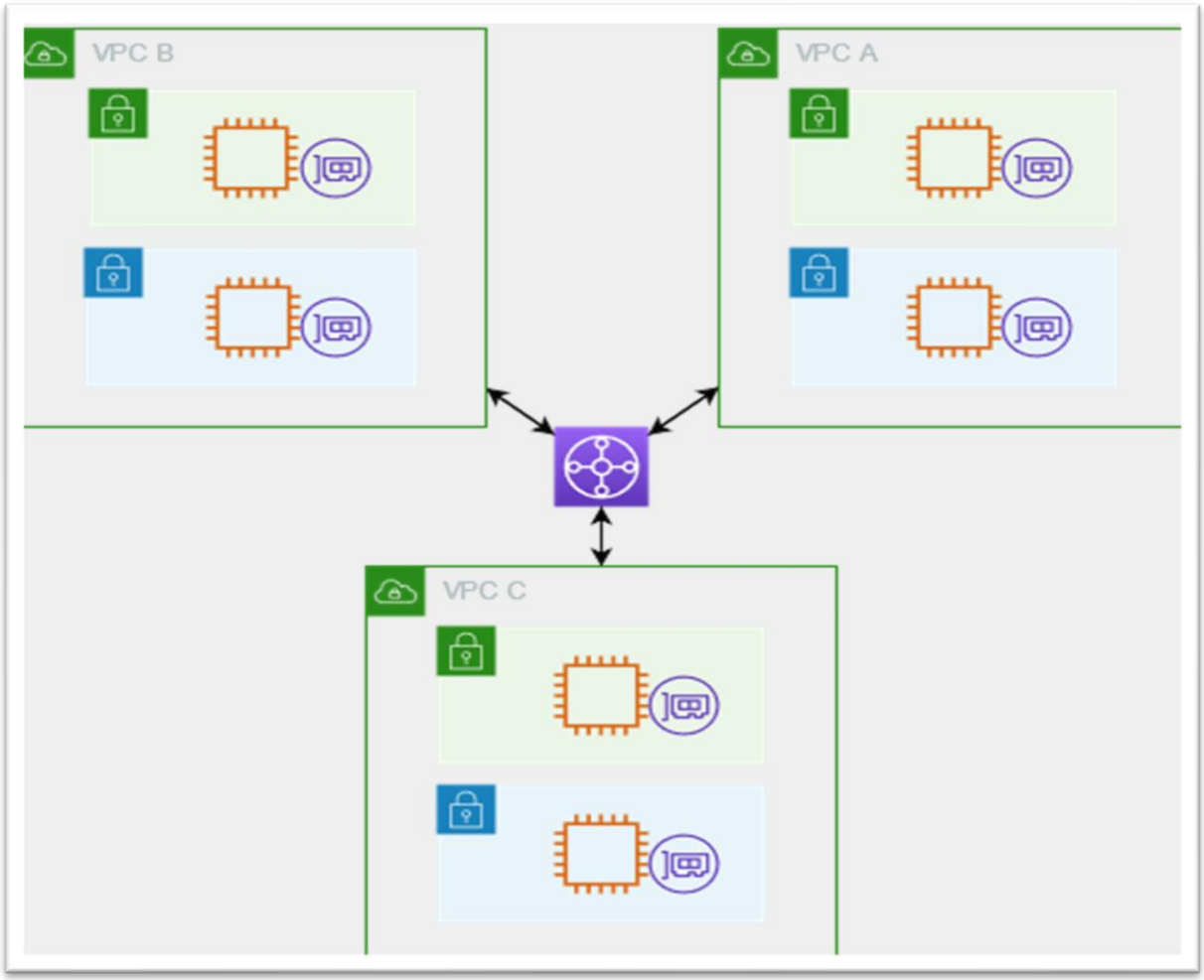
- **Delete a S3 Bucket Object in AWS Cli Command.**
  - aws S3 rm S3://Bucket-name/Object-name

- **List Bucket & Object in AWS Cli Command.**
  - aws s3 ls --------(Show Bucket)
  - aws s3 ls s3://Bucket-name --------(Show Bucket Object)

- Transit Gateway: -

- A transit gateway is a network transit hub that you can use to interconnect your virtual private clouds (VPCs) and on-premises networks. As your cloud infrastructure expands globally, inter-Region peering connects transit gateways together using the AWS Global Infrastructure.

- A transit gateway connect multiple of VPCs in different AWS account.



Transit Gateway in one AWS account in one Region

Step 1: - Create 3 VPCs

Step 2: - Create subnet in All VPCs

Step 3: - Create Particular VPCs Internet Gateway and Attach to VPCs

Step 4: - Attach internet gateway to Route Table

Step 5: - Create Transit Gateway

VPC → Transit gateway → Create → Name → Type ASN (45000000000) → Select Auto Accept Share Attachment Box → Create

Step 6: - Create Transit Gateway Attachment in VPC1 VPC2 VPC3

VPC → Transit Gateway Attachment → Name → Select transit gateway ID

→ Attachment type Select (VPC) → Select VPC ID →Create

Step 7: - Create 3 Instance in Different VPCs

Step 8: - Add Routes in VPCs Route table

- **VPC-1 → RT-1** → Add →VPC 2 & VPC 3 CIDR → Select Destination
  (Transit Gateway) → Save
- **VPC-2 → RT-2** → Add →VPC 1 & VPC 3 CIDR → Select Destination
  (Transit Gateway) → Save
- **VPC-3 → RT-3** → Add →VPC 1 & VPC 2 CIDR → Select Destination
  (Transit Gateway) → Save

Step 9: - Add Inbound Rule in Instances Security Group

- **Instance 1 → SG** → Add → Select (Custom ICMP – IPV4) → Add VPC 2
  - VPC 3 CIDR → Save
- **Instance 1 → SG** → Add → Select (Custom ICMP – IPV4) → Add VPC 2
  - VPC 3 CIDR → Save

- **Instance 1 → SG** → Add → Select (Custom ICMP – IPV4) → Add VPC 2
    - VPC 3 CIDR → Save

Step 10: - Take SSH and PING the Connection and Jump the Private Server And PING, the Connection.

Transit Gateway in Multiple AWS account

Step 1: - Create VPCs All Setup in AWS Account(A) & Account(B)

Step 2: - Create Transit Gateway in Account (A)

Step 3: - Share Transit Gateway {Account(A) to Account(B)}

Select Transit Gateway → Action → Share transit gateway → Create Resource Share → Name → Select Resource Type (Transit gateway) → select TG ID → Select Resource → Next → Next → Allow Sharing with anyone → Select principal type (AWS Account) → Type Receiver Account ID (B) → Add → Create

Step 4: - Account (B) Accept the Resource Share

Resource Share Management (RAM) → Resource share Select → Add

Step 5: - In Account (B) Create a Transit Gateway Attachment

Create Attachment → Name → Select Transit gateway ID → Select

Type VPC → Select Account (B) VPC ID → Create

Step 6: - In Account (A) Create a Transit Gateway Attachment

Create Attachment → Name → Select Transit gateway ID → Select

Type VPC → Select Account (A) VPC ID → Create

Step 7: - Create Instance Account (A) & Account (B)

Step 8: - Add Route on Route Table in Account (A) & Account (B)

- **Account (A)** → RT → Add → Destination {Account (B) VPC CIDR}
  → Target (Transit gateway) → Save
- **Account (B)** → RT → Add → Destination {Account (A) VPC CIDR}
  → Target (Transit gateway) → Save

Step 9: - Add Inbound Rule in Security Group {Account (A) & Account (B)}

- Account (A) → SG → Edit inbound rule → Select Type (All ICMP–IPV4)
  → Type Account (B) VPC CIDR → Save
- Account (B) → SG → Edit inbound rule → Select Type (All ICMP–IPV4)
  → Type Account (A) VPC CIDR → Save

Step 10: - Take SSH and PING the Connection.

- **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 the following locations: Amazon CloudWatch Logs, Amazon S3, or Amazon Kinesis Data Firehose. After you create a flow log, you

can retrieve and view the flow log records in the log group, bucket, or delivery stream that you configured.

Select VPC → Action → Create Flow Log → Name → Filter (All) → Maximum aggregation interval (10 min) → Destination (AWS s3 Bucket) → Type s3 Bucket ARN → log record Format (AWS "default" format) → Log File Format (Text Default) → Partition logs by time (Every 24 Hours) → Create