**AWS HOMEWORK**

**Indroduction**

1. **What is cloud computing?**

**Ans**:- Cloud Computing is where, various servers, applications, other resources are linked(attached) to eachother and provided as a service over the internet.

1. **Service model in cloud?**

**Ans:-** Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) are the three service models of cloud computing

1. **Architecture of Cloud Computing?**

**Ans:-** Cloud architecture makes sense where various cloud related components, such as hardware, virtual resources, software , and virtual network systems interact linked and connect to create cloud computing nature.

1. **Why do we use region in AWS?**

**Ans:-** Region is geographical area which consist of many availability zones consist of data centre . To provide scalability, relatability time consumption and cost cutting we use region .

1. **What is resource in AWS?**

**Ans)** Resource in aws is a thing where we works with. Resources include S3 bucket , EC2 instance ,IAM ,etc

**IAM SERVICE**

1. **How many resources do we have in aws ?**

**Ans:-** We have 170 services with 830 resources in aws

1. **Deployment model in AWS ?**

**Ans:-** There are 3 basic deployment models. SaaS — Software as a Service. IaaS — Infrastructure as a Service. PaaS — Platform as a Service.

1. **Identities in aws ?**

**Ans:-** Identity is identity code varies from user to user an dit provides access to an AWS account

1. **What is IAM user in AWS?**

**Ans:-** IAM user is user that is created in aws to interact with aws services and resources

1. **What is IAM Group in AWS?**

**Ans:-** An IAM group is an identity that consist of collection of IAM users.

1. **What is IAM Policy in AWS?**

**Ans :-** IAM policies can be defined as permissions

1. **What is IAM Role in AWS?**

**Ans:-** IAM roles provide a way to access to AWS with specific permission

1. **Where do we attach Identity based policy ?**

**Ans :-** We attach identity based policy to user and group level. It defines what actions that can perform on AWS resources.

1. **Where do we attach Resource based policy ?**

**Ans :-** We attach Resource based policy to resource itself. It helps to control who can have access perform actions on AWS resources.

1. **Can we able to create Policy via JSON code ?**

**Ans : -** Absolutely you can create Policy through JSON code also . It is a script which helps in structuring data and for creating policies in AWS. You can define permissions and access control in JSON code an then attach this policy to resource or indentity .It is very powerful to manage permissions in AWS

1. **What is Dominator Policy ?**

**Ans :-** ARN stands for Amazon Resource Name. It is unique identifier used in AWS to identify resources such as S3 bucket, IAM roles, EC2 insatnces and many more.

1. **How many types of ARN partition ?**

**Ans :-** There are 3 types of ARN partition

1.aws-cn – for china

2.aws-us-gov – for us gov

3.aws – for standard aws

1. **What are Tags in AWS ?**

**Ans:-** Tags gives additional info about resources . It can be used to organize, manage, or categorize resources. It can be applied to various resources such as S3 buckets, RDS databases, EC2 instances.

1. **What are the fields in ARN ?**

**Ans :-** 1.ARN 2.Partition

3. Service 4.Region

5. Acc id 6. Resource id

**S3 SERVICE**

1. **Difference between Block Storage & Object Storage?**

|  |  |
| --- | --- |
| Block storage | Object Storage |
| 1. It is like Hard disk divided into fixed size blocks for storing data or databases or operating system | 1. It is a like big bucket where we can store files and objects |
| 1. In BS we have direct control over each block and we can read and right to them | 2) In OS each object has it own unique identifier that can be accessed over the internet through APIs |
| 1. It is used when we need low-level access to data | 3) It is used when we need high level access to data |

1. **Difference between Static Website and Dynamic website?**

|  |  |
| --- | --- |
| Static Website | Dynamic Website |
| 1. In Static website all contents remains same for all visitors | 1. In Dynamic website contents changes regularly on user interactions |
| 1. Contents only changes when someone updates or edits the page | 1. Pages contain server side code and it allows server to generate unique content when page is loaded |
| 1. Static website is faster to9 load | 1. Dynamic website is slower to load |

1. **What is major resource of S3 bucket?**

**Ans:** - The major resource of S3 bucket is storage. S3 bucket provides storage for images

Videos, documents, backups. We can store and retrieve data from s3 buckets using

AWS management console, AWS CLI or through APIs

1. **Why do we need to host Static website instead of dynamic website?**

**Ans:** - There are many things that matters most here I .e Simplicity, fast performance, Security, costing, etc

1. **What is versioning? Why do we need versioning?**

**Ans: -** Versioning means keeping multiple versions of files or documents.

Each versioning has unique identifier i.e number

\***Need of Versioning**

**a)** If we accidentally delete the file,versioning helps to recover the file or document

**b)** If we accidentally overwrite the file or some mistake in made in file we can revert the file .

**c)**Many peoples can work on same file at a time becoz of versioning

**d)**  It helps for maintaining control and organization over file and projects

1. **What are the types of objects that we are uploading in s3 bucket ?**

**Ans:-** Images, documents, files, videos and even codes are the various types of objects uploading in s3.

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

**Ans:-** Because it adds extra layer of security to S3 bucket. It helps to protect file from accidental and unauthorized deletion and without proper authorization.

1. **What are the storage classes in Amazon S3**

**Ans:-** In Amazon S3, there are different storage classes based on your needs. IT include Standard, Intelligent-Tiering, Standard-IA (Infrequent Access), One Zone-IA, Glacier, and Glacier Deep Archive. Each class has different characteristics and pricing, so you can pick anyone of them based on your budget and requirement.

1. **What is S3 Multipart upload ?**

**Ans:-** S3 Multipart Upload is a feature in Amazon S3 that allows you to upload large files in parts. Instead of uploading the entire file at once, it breaks it into smaller parts and uploads them concurrently. This method is useful for improving upload speed, and handling large files!

1. **What is ACL?**

**Ans :-** ACL stands for Access Control List. It's a way to manage permissions and control access to your resources in Amazon S3. With ACL, you can specify who can read, write, or delete objects in your S3 bucket.

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

**Ans:-** A lifecycle policy is a feature in Amazon S3 that allows you to define rules for automatically managing the lifecycle of your objects.. For example, you can set rules to automatically transition objects to a different storage class after a certain period of time or to expire objects after a specific duration.

Using a lifecycle policy helps you optimize storage costs and improve performance by automatically moving objects to the most appropriate storage class based on their lifecycle. It also helps you meet compliance requirements by automatically deleting or archiving objects when they are no longer needed.

1. **How can we make our bucket public ?**

**Ans:-** To make your bucket public in Amazon S3, you can modify the bucket's access control list (ACL) or use a bucket policy. By granting public read access, anyone can access the objects in your bucket. However, please note that making a bucket public means that all objects in the bucket will be accessible to the public

1. How can we give public access to our bucket ?

Ans :- To give public access to your bucket in Amazon S3, you can follow these steps:

1. Go to the S3 Management Console.

2. Select the bucket for which you want to grant public access.

3. Click on the "Permissions" tab.

4. Under the "Public access" section, click on "Edit".

5. Choose the desired level of public access based on your requirements.

- If you want to make the entire bucket public, select "Public" for both "Bucket access" and "Objects" options.

- If you want to make only specific objects public, select "Public" for "Bucket access" and "Private" for "Objects".

1. **Aws pricing factor of the S3 Service**

**Ans:-** The pricing of Amazon S3 (Simple Storage Service) is based on a few factors:

1. Storage: You are charged based on the amount of data you store in your S3 bucket. The pricing varies depending on the storage class you choose, such as Standard, Intelligent-Tiering, Glacier, etc.

2. Requests: You are also charged for the number of requests you make to your S3 bucket, including GET, PUT, COPY, and LIST requests.

3. Data Transfer: If you transfer data between your S3 bucket and other AWS services or the internet, there may be additional charges for data transfer.

4. Data Transfer Acceleration: If you enable Data Transfer Acceleration, which speeds up data transfers to and from S3, there may be additional charges.

5. Storage Management: If you use features like S3 Inventory, S3 Analytics, or S3 Object Tagging, there may be additional charges for storage management.

1. **How can we configure the static website logs in s3 ?**

**Ans:-** To configure static website logs in S3, you can follow these steps:

1. Enable server access logging: Go to the properties of your S3 bucket hosting the static website and enable server access logging.

2. Set up a target bucket: Create another S3 bucket where you want to store the access logs.

3. Configure logging settings: In the properties of your S3 bucket hosting the static website, find the logging section and specify the target bucket

4. Access and analyze logs: Once logging is enabled, S3 will start generating access logs in the specified target bucket.

**16. What is CORS ?**

**Ans:-** CORS, which stands for Cross-Origin Resource Sharing, is a way for web browsers to securely share resources (like data or files) between different domains. It allows websites to control which domains are allowed to access their resources

**17. What is S3 Inventory ?**

**Ans:-** S3 Inventory is a feature in Amazon S3 that allows you to generate a report of metadata about objects in your S3 buckets. It provides information like object keys, sizes, storage classes, and encryption status.

**18. What does it mean by Requester pays ?**

**Ans :-** Requester pay in Amazon S3, it means that the person or entity making the request for data transfer or retrieval from an S3 bucket is responsible for the associated costs. Normally, the bucket owner incurs all costs related to data transfer and retrieval. However, with the "Requester pays" feature enabled, the requester takes on the financial responsibility for those operations..

**19. What is The secondary word for "Transfer acceleration"**

**Ans :-** The secondary word for "Transfer acceleration" is "Speed up." It refers to the feature in Amazon S3 that allows you to accelerate the transfer of data to and from your S3 bucket by using the Amazon CloudFront global network

**20. Why do we need to use this transfer acceleration ?**

**Ans:-** Transfer Acceleration can be beneficial in scenarios where you need to transfer large amounts of data to and from your Amazon S3 bucket quickly. In transfer acceleration this large data in fixed in smaller data packs and to increase the speed of transfer of data.

**AWS Cloud Trail**

1. **What is AWS CloudTrail?**

**Ans:-** AWS CloudTrail is a service provided by Amazon Web Services (AWS) that allows you to monitor and log all the API activity in your AWS account. It records events such as API calls, resource modifications, and account activity, and stores them in an S3 bucket or delivers them to CloudWatch Logs. CloudTrail provides valuable insights into who accessed your resources, what changes were made, and when they occurred.

**2.) What is the exact purpose of enabling CloudTrail ?**

**Ans :-** It enhances security by recording events such API activities in our aws account. By enabling it this logs are then stored in s3 bucket and further are used for troubleshooting operational analysis and helping to identify the root cause of issue. In short it makes aws more secure and well managed.

**3.) Explain how we can create a trail in aws cloud trail ?**

**Ans :-** Sure! To create a trail in AWS CloudTrail, you can follow these steps:

1. Open the AWS Management Console.

2. Go to the CloudTrail service.

3. Click on "Trails" in the left navigation pane.

4. Click on the "Create trail" button.

5. Give your trail a name and choose the AWS S3 bucket where you want to store your trail logs.

6. Configure the settings for your trail, such as whether you want to include global services or specific regions.

7. Enable log file validation if desired.

8. Choose the CloudWatch Logs group and stream for your trail logs.

9. Optionally, you can add tags to your trail for better organization.

10. Review your settings and click on "Create trail" to create your trail.

That's it! Your trail will now start capturing and storing logs of the activities happening in your AWS account.

**4.) How can we enable logging for S3 bucket using cloud trails ?**

**Ans :-** To enable logging for an S3 bucket using CloudTrail, you can follow these steps:

1. Open the AWS Management Console.

2. Go to the CloudTrail service.

3. Click on "Trails" in the left navigation pane.

4. Select the trail that you want to enable logging for.

5. Click on "Edit" to modify the trail settings.

6. Scroll down to the "Data events" section and click on "Add S3 bucket."

7. Choose the S3 bucket for which you want to enable logging.

8. Click on "Save" to update the trail settings.

Once you've completed these steps, CloudTrail will start logging data events for the selected S3 bucket.

**5.) How do you get the list of all created trailers in your production account ?**

**Ans:-** To get the list of all created trails in your production account, you can follow these steps:

1. Open the AWS Management Console.

2. Go to the CloudTrail service.

3. Click on "Trails" in the left navigation pane.

Here, you will see a list of all the trails that have been created in your production account. You can view the details of each trail, such as the trail name, the S3 bucket where the logs are stored, and the status of the trail.

**6.) Can we create a trail for a multi region, if yes then how can we configure it ?**

**Ans:-** Yes, you can create a trail for multiple regions in AWS CloudTrail. Here's how you can configure it:

1. Open the AWS Management Console.

2. Go to the CloudTrail service.

3. Click on "Trails" in the left navigation pane.

4. Select the trail for which you want to enable multi-region logging or create a new trail.

5. In the trail settings, scroll down to the "Management events" section.

6. Toggle the switch for "Multi-Region" to enable multi-region logging.

7. Choose the regions for which you want to capture management events.

8. Click on "Save" to update the trail settings.

**7.) What is cloud trail event history ?**

**Ans :-** CloudTrail Event History is a feature of AWS CloudTrail that provides a detailed record of events and API activity within your AWS account. It captures information about actions taken on AWS resources, such as creating or modifying instances, accessing S3 buckets, or making changes to security groups.

The Event History allows you to view, search, and analyze the recorded events in your AWS account. It provides insights into who performed specific actions, when they occurred, and the resources that were affected.

You can access the CloudTrail Event History through the AWS Management Console or programmatically using the AWS SDKs or APIs.

SNS

**1. What is SNS ?**

**Ans:-** SNS stands for Amazon Simple Notification Service. It is a messaging service provided by Amazon Web Services (AWS). SNS enables you to send notifications to individuals or groups via multiple channels such as email, SMS, mobile push notifications, and more.

SNS is often used for various use cases, including sending alerts, broadcasting messages, and triggering actions based on events

**2.Why do we use SNS ?**

**Ans:-** We use SNS for a variety of reasons. It allows us to easily send notifications and messages to individuals or groups through different channels like email, SMS, and mobile push notifications. SNS helps us keep our users informed, engaged, and updated with important information or events. So, in short, we use SNS to effectively communicate with our users and deliver important messages across various platforms and devices.

**3.What is SNS Mobile Push ?**

**Ans:-** SNS Mobile Push refers to the mobile push notification feature provided by Amazon Simple Notification Service (SNS). It allows you to send push notifications to mobile devices, such as smartphones and tablets, through various platforms like iOS, Android, and Kindle Fire.

With SNS Mobile Push, you can engage with your app users by sending them real-time notifications. These notifications can contain relevant information, updates, or alerts that you want to communicate to your users.

To use SNS Mobile Push, you need to have SDK (Software Development Kit) into your mobile app. This SDK provides the functionality to register devices, manage subscriptions, and send push notifications. You can then use the SNS console or API to configure and send push notifications to the registered devices.

**4. What are FIFO topics on SNS**

**Ans:-** FIFO topics in Amazon SNS refer to First-In-First-Out topics.

When you use a FIFO topic, the order in which messages are published is preserved, and subscribers receive the messages in the same order. This is especially useful for scenarios where message order is critical, such as processing financial transactions or maintaining a sequential workflow.

To create a FIFO topic, you need to specify a topic name that ends with the ".fifo" suffix. For example, "my-topic.fifo".

It's important to note that FIFO topics have some additional requirements and limitations compared to standard topics in Amazon SNS. For example, you need to specify a message deduplication ID for each message, and the maximum message size is slightly smaller.

**5. What is 10DLC in AWS ?**

**Ans:-** 10DLC in AWS stands for 10-Digit Long Code. It is a messaging service that allows businesses to send application-to-person (A2P) messages using standard 10-digit phone numbers. This service is particularly useful for businesses that want to send text messages to their customers at scale, such as appointment reminders, marketing messages, or notifications.

By using 10DLC, businesses can benefit from improved message deliverability, reduced costs, and increased flexibility compared to traditional A2P messaging methods

6. Difference between Amazon SNS & Amazon SQS

|  |  |
| --- | --- |
| Amazon SNS | Amazon SQS |
| 1.Amazon SNS is a publish-subscribe messaging service.  2. It allows you to send messages to multiple subscribers (such as email, SMS, or HTTP endpoints) simultaneously | 1.Amazon SQS is a fully managed message queuing service  2. SQS works on the principle of queues, where messages are sent to a queue by producers and then retrieved and processed by consumers |

Ans:-

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

**Ans:-** 1. HTTP/HTTPS: You can send messages as HTTP or HTTPS POST requests to an endpoint of your choice. This allows you to integrate SNS with your own applications or services.

2. Email: SNS can deliver messages to email addresses. Subscribers can receive notifications in their email inbox.

3. SMS: SNS supports sending messages as SMS (Short Message Service) to mobile devices. This is useful for sending important notifications or alerts directly to subscribers' phones.

4. Mobile Push Notifications: SNS can send push notifications to mobile devices using platforms like Apple Push Notification Service (APNS), Google Cloud Messaging (GCM), Firebase Cloud Messaging (FCM), and others. This allows you to reach users on their smartphones or tablets.

**8. On which delivery method do we use and configure the subscription ?**

**Ans:-** To configure a subscription and specify the delivery method in AWS SNS, you would use the AWS Management Console or the AWS SDK/API

For example, if you want to configure an email subscription, you would specify the email address as the endpoint for the subscription. Similarly, if you want to configure an HTTP/HTTPS subscription, you would provide the endpoint URL to which SNS should send the messages.

EC2

**1.What is EC2, Why do we need EC2 service in cloud computing ?**

**Ans:-**

EC2 stands for Elastic Compute Cloud, and it's a service provided by Amazon Web Services (AWS) in cloud computing. It's basically a virtual server in the cloud that you can use to run applications and store data.

It offers scalability, flexibility and cost effectiveness.

With EC2, we can easily adjust our computing resources based on our needs. This means we can quickly add or remove instances as our workload changes, ensuring performance and efficiency. Plus, EC2 allows us to pay only for the resources we use, saving us money in the long run.

**2.Features of Amazon EC2 ?**

**Ans:-**

1. Scalability: EC2 allows you to easily scale your computing resources up or down based on your needs. You can quickly add or remove instances to handle changes in workload.

2. Flexibility: You have full control over your virtual server instances. You can choose the operating system, configure networking and security settings, and even customize the hardware specifications.

3. Cost-Effectiveness: With EC2, you only pay for the resources you actually use. This means you can optimize costs by scaling resources as needed

5. Security: EC2 offers various security features, including firewalls, encryption, and network isolation, to protect your applications and data.

6. Integration: EC2 seamlessly integrates with other AWS services, such as Amazon S3 for storage, Amazon RDS for databases, and Amazon VPC for networking.

**3.What is Hypervisor ? and its types ?**

:**Ans :-** A hypervisor is a software or hardware component that allows multiple virtual machines (VMs) to run on a single physical server.

There are two main types of hypervisors:

1. Type 1 (Bare Metal): This type of hypervisor runs directly on the physical hardware, without the need for an underlying operating system. It provides direct access to the server's resources. Examples include VMware ESXi and Microsoft Hyper-V.

2. Type 2 (Hosted): This hypervisors run on top of an existing operating system. They rely on the host operating system to manage hardware resources. These are commonly used for desktop virtualization or testing environments. Examples include Oracle VirtualBox and VMware Workstation.

**4. Where we use hypervisor?**

**Ans:-** We use hypervisors in various scenarios. Some common use cases include:

1. Desktop Virtualization: Hypervisors can be used to create virtual desktop infrastructure (VDI), allowing multiple users to access their own virtual desktops from a central server.

2. Testing and Development: Hypervisors provide a convenient and isolated environment for software testing and development. Developers can create multiple virtual machines with different configurations to test their applications or simulate different environments.

3. Cloud Computing: Many cloud service providers use hypervisors to offer Infrastructure-as-a-Service (IaaS) solutions. They create and manage virtual machines for their customers, who can then run their applications and services in the cloud.

**5. Steps to create EC2 Instance**

**Ans:-** Sure, I can help you with that! Here are the steps to create an EC2 instance in AWS:

1. Sign in to the AWS Management Console.

2. Open the Amazon EC2 console.

3. Click on "Launch Instance" to start the instance creation process.

4. Choose an Amazon Machine Image (AMI) - this is the operating system and software configuration for your instance.

5. Select an instance type - this determines the hardware specifications of your instance.

6. Configure the instance details, such as the number of instances, network settings, and storage options.

7. Add any additional storage volumes or tags as needed.

8. Configure security groups - these control inbound and outbound traffic to your instance.

9. Review your instance configuration and make any necessary changes.

10. Finally, click on "Launch" to create your EC2 instance.

**6. How many types of EC2 Instance-State codes ?**

**Ans:-** There are a few different types of EC2 instance state codes that represent the current state of an instance. \ones:

1. "0" - Pending: The instance is in the process of being launched.

2. "16" - Running: The instance is up and running.

3. "32" - Shutting Down: The instance is being shut down or terminated.

4. "48" - Terminated: The instance has been successfully terminated and no longer exists.

5. "64" - Stopping: The instance is in the process of being stopped.

6. "80" - Stopped: The instance is stopped and can be started again.

**7. What is KMS ?**

**Ans:-** KMS stands for Key Management Service. It's a service provided by AWS (Amazon Web Services) that helps you create and manage encryption keys. With KMS, you can generate, store, and control the encryption keys used to encrypt your data. This helps you protect your data.

**8. AWS Amazon EC2 Instance types ?**

**Ans:-** There are several types of Amazon EC2 instances available to meet different computing needs. Some common instance types include:

1. General Purpose (e.g., t3, m5) - Balanced compute, memory, and networking resources.

2. Compute Optimized (e.g., c5) - High-performance compute instances for CPU-intensive workloads.

3. Memory Optimized (e.g., r5) - Instances with high memory capacity for memory-intensive applications.

4. Storage Optimized (e.g., i3, d2) - Instances optimized for high-speed, low-latency storage.

5. GPU Instances (e.g., p3, g4) - Instances with powerful GPUs for graphics-intensive and parallel computing workloads.

6. FPGA Instances (e.g., f1) - Instances with field-programmable gate arrays for custom hardware acceleration.

7. ARM-based Instances (e.g., a1) - Instances powered by AWS Graviton processors for cost-effective performance.

**9. How many types of status checks happen in aws ?**

**Ans:-.** The two main types are the system status check and the instance status check. The system status check monitors the underlying infrastructure, while the instance status check monitors the instance itself.

**10. What are EBS Volumes and its types ?**

**Ans:-** EBS volumes in AWS are virtual hard drives that you can attach to your EC2 instances. They provide persistent block-level storage and can be used for storing data, running databases, or hosting applications.

There are several types of EBS volumes available:

1. General Purpose SSD (gp2): This is the default volume type and offers a balance of price and performance for a wide range of workloads.

2. Provisioned IOPS SSD (io1): This volume type is designed for high-performance applications that require low-latency and consistent I/O performance.

3. Throughput Optimized HDD (st1): This volume type is optimized for frequently accessed, throughput-intensive workloads, such as big data processing or log processing.

4. Cold HDD (sc1): This volume type is designed for less frequently accessed workloads, providing low-cost storage for infrequently accessed data.

5. Magnetic (standard): This is the oldest volume type and offers the lowest cost per gigabyte, but has lower performance compared to other types.

**11. Purpose of Using EBS volumes ?**

**Ans:-** EBS volumes are used for various purposes in AWS.

1. Data Storage: EBS volumes are ideal for storing data that needs to persist even if the associated EC2 instance is stopped or terminated. You can store files, documents, databases, and other types of data on EBS volumes.

2. Database Hosting: EBS volumes are commonly used to host databases like MySQL, PostgreSQL, or Oracle. The data stored on EBS volumes can be accessed by the database server, providing reliable and scalable storage for your databases.

3. Application Hosting: EBS volumes are also used to host applications. You can install your application software on an EC2 instance and store the application data on an EBS volume.

4. Disaster Recovery: EBS volumes can be used for disaster recovery purposes. By taking snapshots of your EBS volumes, you can create backups of your data and restore it in case of any data loss or system failure.

**12. How many types of purchasing options do we have in aws ec2 ? (\*\*\*\*\*\*\*)**

**Ans:-** In AWS EC2, there are three types of purchasing options available for instances:

1. On-Demand Instances: With on-demand instances, you pay for compute capacity by the hour or second, with no long-term commitments or upfront costs. This option provides flexibility and allows you to scale your instances up or down based on your needs.

2. Reserved Instances: Reserved instances provide a significant discount compared to on-demand instances. You commit to using the instance for a specific term (1 or 3 years) and in return, you receive a lower hourly rate. Reserved instances are suitable for applications with steady-state or predictable usage.

3. Spot Instances: Spot instances offer the ability to bid on unused EC2 capacity and can provide significant savings compared to on-demand instances. However, spot instances are subject to availability and can be terminated by AWS with a short notice period if the spot price exceeds your bid price.

**13. What is NIC & it’s types ?**

**Ans:-** NIC stands for Network Interface Card. It is a hardware component that allows a computer or device to connect to a network. A NIC is responsible for facilitating the transmission and reception of data between the device and the network.

1. Ethernet NIC: This is the most common type of NIC and is used to connect devices to Ethernet networks. It typically has an RJ-45 port for connecting an Ethernet cable.

2. Wireless NIC: Also known as a Wi-Fi adapter, this type of NIC enables devices to connect to wireless networks. It uses radio waves to transmit and receive data without the need for physical cables.

3. Fiber NIC: Fiber NICs are used for connecting devices to fiber optic networks. They have fiber optic connectors, such as SC or LC, which allow for high-speed data transmission over long distances.

4. Bluetooth NIC: Bluetooth NICs are used for connecting devices wirelessly over short distances. They are commonly found in devices like smartphones, laptops, and Bluetooth-enabled peripherals.

**14. What is elastic IP ? & WHY were we used ?**

**Ans:-** An elastic IP (EIP) is a static, public IPv4 address provided by AWS. It can be associated with your EC2 instances or certain other AWS resources.

Elastic IPs are used for various reasons:

1. Static IP: EIPs provide a fixed, public IP address that remains the same even if you stop or start your EC2 instance. This is useful if you need a consistent IP address for your application or if you want to access your instance remotely.

2. IP Whitelisting: Many applications and services require you to whitelist specific IP addresses for security purposes. With an EIP, you can assign a fixed IP address to your instances and easily update your firewall rules or access controls.

3. Elastic IP Mobility: If you need to replace an EC2 instance, you can quickly and easily reassociate the EIP with the new instance. This allows your application or service to maintain the same public IP address without any downtime.

4. Internet Gateway: Elastic IPs are also used in conjunction with an internet gateway to enable communication between your VPC (Virtual Private Cloud) and the internet.

**15. What is the snapshot of why we use it in aws**

**Ans:-** In AWS, a snapshot is a point-in-time copy of an Amazon EBS volume. It captures the data and configuration of the volume at the time the snapshot is taken.

Snapshots are used for various purposes:

1. Data Backup: Snapshots provide a way to back up your EBS volumes. By taking snapshots, you can create a copy of your data that can be used to restore the volume in case of data loss or to create new volumes with the same data.

2. Data Replication: Snapshots can be used to replicate data across different regions or accounts. You can copy snapshots to different regions and use them to create new volumes in those regions, allowing for data redundancy and disaster recovery.

3. Volume Modification: Snapshots can be used to modify the configuration of an EBS volume. You can create a snapshot of a volume, make changes to the snapshot (such as resizing the volume), and then create a new volume from the modified snapshot.

4. Testing and Development: Snapshots can be used to create new volumes for testing and development purposes. You can create a snapshot of a production volume, use it to create a new volume, and then perform testing or development activities without impacting the production environment.

16. What is the lifecycle manager in snapshot ?

Ans:- The Snapshot Lifecycle Manager in AWS is a feature that allows you to automate the management of your EBS snapshots. It provides you with a way to define rules and policies for snapshot creation, retention, and deletion.

With the Snapshot Lifecycle Manager, you can set up policies based on time or usage to automate the creation and deletion of snapshots. For example, you can create a policy to take a snapshot every 24 hours or every week. You can also define how long you want to retain the snapshots before they are automatically deleted.

**17. what are the types of the Scaling option ?**

**Ans:-** In general, there are two common types of scaling options: vertical scaling and horizontal scaling.

1. Vertical Scaling (also known as scaling up): This involves increasing the resources (such as CPU, memory, or storage) of an individual server or instance. It is done by upgrading to a higher-capacity machine. Vertical scaling is suitable when the workload requires more power from a single server.

2. Horizontal Scaling (also known as scaling out): This involves adding more servers or instances to distribute the workload. Instead of increasing the resources of a single server, horizontal scaling focuses on adding more servers to handle the increased load. It is commonly used in scenarios where the workload can be divided across multiple servers.

**18. What is the desired capacity in ASG**

**Ans:-** In the context of an Auto Scaling Group (ASG), the desired capacity refers to the number of instances that you want the ASG to maintain at any given time. It represents the ideal number of instances that should be running to handle the workload efficiently.

When you set the desired capacity for an ASG, the Auto Scaling service automatically adjusts the number of instances to match that desired capacity. It can scale up or down based on factors like CPU utilization, network traffic, or custom metrics.

**19. What is the target group ?**

**Ans:-** In AWS, a target group is a component of Elastic Load Balancing (ELB) that helps distribute incoming traffic across multiple instances or containers. It acts as a logical grouping of targets, such as EC2 instances, ECS tasks, or Lambda functions, that can receive traffic from a load balancer.

When you create a target group, you specify the target type (instances, IP addresses, or Lambda functions) and the protocol and port for the traffic. The target group then acts as a routing destination for the load balancer.

Target groups are used in conjunction with load balancers, such as Application Load Balancers (ALB) and Network Load Balancers (NLB).

**20. What is the group of LB**

**Ans:-** The group of LB refers to the Load Balancer. In AWS, there are different types of load balancers available, such as Application Load Balancer (ALB), Network Load Balancer (NLB), and Classic Load Balancer (CLB). These load balancers help distribute incoming traffic across multiple targets, such as instances or containers, to ensure high availability and scalability.

Each load balancer type has its own unique features and use cases. For example, ALB operates at the application layer (Layer 7) and is ideal for HTTP and HTTPS traffic, while NLB operates at the transport layer (Layer 4) and is suitable for handling TCP and UDP traffic.

**21. What is the threshold ?**

**Ans:-** Tthresholds help define the boundaries or conditions for certain actions or decisions to be taken based on specific values or criteria.

For example, in the context of monitoring and alerting systems, a threshold can be set to monitor the CPU utilization of a server. If the CPU utilization exceeds a certain threshold, it can trigger an alert or initiate an automated response to address the high resource usage.

**22. What is a Health Check ?**

Ans:- In AWS, a health check refers to a feature provided by the Elastic Load Balancing service. When you configure a load balancer, you can set up health checks to monitor the health and availability of the registered instances or targets.

The health check in AWS periodically sends requests to the instances or targets to check if they are responding properly. It can be configured to use different protocols, such as HTTP, HTTPS, TCP, or SSL, depending on the type of load balancer being used.

**23. What is ASG ? & Its types ?**

Ans:- ASG stands for Auto Scaling Group. It is a feature provided by AWS (Amazon Web Services) that allows you to automatically adjust the number of instances in a group based on the demand or load of your application.

There are different types of Auto Scaling Groups in AWS:

1. On-Demand Instances: This type of Auto Scaling Group uses instances that are provisioned on-demand, meaning they are launched and terminated as needed based on the scaling policies and demand.

2. Spot Instances: Spot Instances are a cost-effective option for Auto Scaling Groups. They allow you to bid on unused EC2 instances, known as "spot instances," and use them in your Auto Scaling Group. Spot instances can be significantly cheaper than On-Demand instances but come with the risk of being interrupted if the spot price exceeds your bid.

3. Scheduled Scaling: With scheduled scaling, you can set up a predefined schedule to adjust the capacity of your Auto Scaling Group. This is useful when you know in advance that your application will experience predictable changes in demand at specific times.

4. Target Tracking Scaling: This type of scaling allows you to set a target value for a specific metric, such as CPU utilization or request count per instance. The Auto Scaling Group will automatically adjust the number of instances to maintain the target value.

**24. Features of Load Balancers ?**

Ans:-

1. High Availability: Load balancers ensure that your applications are highly available by distributing traffic across multiple servers. If one server fails, the load balancer automatically redirects traffic to the remaining healthy servers, minimizing downtime.

2. Scalability: Load balancers help you scale your applications horizontally by adding or removing servers based on demand. As the traffic increases, the load balancer can dynamically add more servers to handle the load. And when the traffic decreases, it can scale down by removing servers, saving costs.

3. Health Checks: Load balancers regularly perform health checks on the servers to ensure they are responsive and available. If a server fails a health check, the load balancer stops sending traffic to it until it becomes healthy again.

4. Session Persistence: Load balancers can maintain session persistence, ensuring that a user's requests are consistently routed to the same server. This is important for applications that require session state or have long-running transactions.

6. Content-Based Routing: Load balancers can route traffic based on specific criteria, such as URL paths or request headers. This allows you to direct requests to different backend servers based on the content or type of request.

7. Load Balancing Algorithms: Load balancers use various algorithms to distribute traffic, such as round-robin, least connections, or weighted algorithms. These algorithms help evenly distribute the load across servers and optimize performance.

**25. What is load balancer and its types ?**

**Ans:-** A load balancer is a device or software that evenly distributes incoming network traffic across multiple servers. It helps optimize resource utilization, improve responsiveness, and ensure high availability of applications or websites. There are a few types of load balancers, including hardware load balancers, software load balancers, and cloud-based load balancers. Each type has its own advantages and is used in different scenarios.

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

**Ans:-**

When a request comes in, the load balancer receives it and then decides which server to send the request to. It does this by using different algorithms, like round-robin, least connections, or IP hash.

Once the load balancer selects a server, it forwards the request to that server, and the server processes the request and sends back the response to the load balancer. The load balancer then sends the response back to the original requester.

The load balancer continuously monitors the servers to check their health and availability. If a server becomes overloaded or goes offline, the load balancer automatically redirects traffic to other servers, ensuring smooth operation and preventing any single server from getting overwhelmed.

**27. What is a key pair, and its types ?**

Ans:- A key pair is a pair of cryptographic keys that are used in various security protocols and systems. It consists of two related keys: a public key and a private key.

The public key is shared with others and is used to encrypt data or verify digital signatures. It can be freely distributed and is often used for encryption and authentication purposes.

On the other hand, the private key is kept secret and should only be known to the owner. It is used to decrypt data that has been encrypted with the corresponding public key or to generate digital signatures. The private key is crucial for maintaining the confidentiality and integrity of the data.

As for the types of key pairs, there are several algorithms used to generate them, such as RSA, DSA, and ECC (Elliptic Curve Cryptography). Each algorithm has its own strengths and characteristics, but they all involve the generation of a public-private key pair.

**28. How many types of volume states do we have ?**

Ans:- There are typically three types of volume states:

1. Available: This means that the volume is not currently attached to any instance and can be attached to an instance if needed.

2. In-use: This state indicates that the volume is currently attached to an instance and is being used by that instance.

3. Deleting: When a volume is being deleted, it enters the deleting state. During this time, the volume is being removed and cannot be attached to any instance.

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

Ans:- You can attach multiple IP addresses to instances, depending on the specific configuration and capabilities of the cloud platform or network setup you are using.

In some cases, you may have the option to assign multiple private IP addresses to an instance.

Additionally, there are also options for assigning multiple public IP addresses or using load balancers to distribute traffic across multiple instances

**30. What are NACL & Its types ?**

**Ans:-** NACL stands for Network Access Control List. It is a security feature used in some network setups to control the traffic flow in and out of subnets or network segments. NACLs act as a firewall at the subnet level, allowing or denying traffic based on rules defined in the NACL configuration.

There are two types of NACLs commonly used:

1. Inbound NACL: This type of NACL controls incoming traffic from external sources into the subnet. It specifies rules for allowing or blocking traffic based on factors like source IP addresses, protocols, and ports.

2. Outbound NACL: On the other hand, the outbound NACL controls outgoing traffic from the subnet to external destinations. It defines rules for allowing or blocking traffic based on factors like destination IP addresses, protocols, and ports.

31.