INTERVIEW PREPARATION

---

1) What is cloud computing:

Answer: -

Cloud computing is the delivery of IT resources over the internet, or "the cloud", on demand. It allows users to access computing services, such as storage, databases, and networking, without having to buy, own, and maintain physical resources.

2) What is Aws:

Answer:

Amazon Web Services (AWS) is a cloud computing platform that offers a range of services to help businesses and organizations become more agile, innovative, and cost-effective. AWS offers a variety of services, including:

- Compute
- Storage
- Databases
- Networking and content delivery
- Analytics
- Machine learning
- Security, identity, and compliance

3) Why Aws in top in market:

Answer:

AWS has significantly more services, and more features within those services, than any other cloud provider–from infrastructure technologies like compute, storage, and databases–to emerging technologies, such as machine learning and artificial intelligence, data lakes and analytics, and Internet of Things.

4) What are the different tenancy models for AWS EC2[Elastic Compute Cloud]?

Answer:

- **Shared Tenancy:** This is the default tenancy model for AWS EC2, which is commonly used. On a physical host, the EC2 instance from different customers can be hosted. When we stop and start our instance, the underlying host gets changed. In case of a reboot, our underlying hardware does not change.
- **Dedicated Tenancy:** This tenancy model ensures that your AWS EC2 instances are running at specific hardware for your account.
  There are 2 different options available under a dedicated tenancy for AWS EC2 instances.
- **Dedicated Host:** With a dedicated host option, you purchase a whole physical host from AWS, and this host comes to you on an hourly basis billing manner similar to ec2 times are billed. For dedicated hosts, even if you stop and start your instances, they will continue to run in the same physical host, which will help you

in reusing any of the existing hardware-bound licenses based on your business requirement. One key thing to note here this tenancy is one of the costliest of all compared to others

- **Dedicated Instances:** With a dedicated instance, you're utilizing the benefits of having separated hosts from the rest of the AWS customers, but you are not paying for the entire host all at go. This type of dedicated instance model is similar to that of the default model, where you are not worried about where the instances are running, but it does ensure they're kept separate from other customers. The most important point that you need to be aware of is if your dedicated instances are using Elastic Block Storage (EBS), those would be on shared hardware.

5) What are Instances, and what are their types?

Answer:

Instances are virtual environments provided by EC2, also known as EC2 Instances, that can be used to host applications by cloud users. Following are the types of Instances available in Amazon EC2:

- **General Purpose**: These instances equalize compute, memory, and networking resources and are ideal for applications that use these resources proportionately, such as web servers and code repositories.
- **Compute Optimized:** These instances benefit from high-performance processors and are suitable for compute-bound applications like gaming servers, ad server engines, and compute-intensive applications.
- **Memory-Optimized:** These instances are ideal for workloads that require the processing of large data sets in memory.
- **Accelerated Computing:** These instances use hardware accelerators, or co-processors, to perform functions, such as calculations, graphics processing, data pattern matching, and others.
- **Storage Optimized:** These instances are widely used to process workloads that require high, sequential read and write access to large data sets on local storage.

6) What is the role of Amazon Virtual Private Cloud (VPC) in the networking landscape?

Answer:

Expect to come across this popular question in AWS solution architect interview questions.
The ideal way to connect from your local data center to your cloud resources is through a VPC. Each of your instances is given a private IP address that may be accessible from your data center after your data center is connected to the VPC where it is located. In this manner, you can use the resources on your public cloud as if they were on your personal network.

7) How do we get billed for AWS Elastic IPs when it is not associated?

Answer:

- For reservation of AWS Elastic IP even though it's not attached to EC2.
- When it is attached to an instance in the stopped state
- Attached to an instance that already has an AWS Elastic IP attached
- Associated with non-attached network interface

8) What is Amazon EC2?

Answer:

EC2 stands for Elastic Cloud Compute. This technology is widely used to scale up computing capacities while eliminating the need for hardware architecture. The Amazon EC2 technology can launch multiple servers and manage security, networking, and storage all at once. Besides, while using EC2, the need for traffic forecast reduces as there are options to scale up and scale down as per the requirements.

9) Do you know what Identity and Access Management are?

Answer:

Identity and Access Management (IAM) is a specialized web service dedicated to securing access to AWS resources. The IAM web service is vital to manage AWS users, access key credentials, and access permissions for AWS resources and applications.

10) What are the features of IAM?

Answer:

The features of IAM are as follows:

- **Shared Access** to our Account helps in sharing resources with the help of the shared access features.
- **Free of cost** - AWS IAM is free to use, and also all the charges are added when we access other Amazon web services using IAM users.
- **Centralized control over your Aws account** - Helps in the new creation of users and groups of any form of cancellation.
- **Grant permission to the user** - It holds administrative rights, and the users can grant permission to access.
- **Multifactor Authentication** - It adds layers of security implemented on our account by a third party.

11) What are the types of IAM policies?

Answer:

AWS policies are of two types:

- **Identity-based policies:** This is the policy that binds with AWS identities, such as a user's, group or role. IAM policies are an example of that. These policies can be either Amazon Web Services managed or customer-managed.
- **Resource-based policies:** AWS resource-based policies are the ones that can be tied directly to Amazon Resources, like a bucket policy (S3). Resource-based policies are only available for certain services.

12) Explain best practices to manage access to AWS resources?

Answer:

- **Do not use root accounts:** Since root accounts have access to all the AWS resources and services, it is not a good idea to share or use them.
- **Use Groups:** Create groups, grant access to them, and add users to them – so that all users within the group have the same access.
- **Enable Multi-factor Authentication (MFA):** MFA should be enabled for privileged users such as admins. MFA adds an additional layer of security.
- **Grant least privileges:** Only grant permissions that are necessary for the user or group.

13) Name the three different types of load-balancers used in Amazon EC2?

Answer:

Different types of load-balancers used in Amazon EC2 are:

- **Application Load Balancer:** Used to make routing decisions at the application layer
- **Network Load Balancer:** Used to make routing decisions at the transport layer
- **Classic Load Balancer:** Used within the EC2-Classic network to balance load at varying EC2 instances.

14) Explain the AWS disaster recovery solution.

Answer:

AWS disaster recovery system enables businesses to quickly recover their critical IT systems without extra investment in a second infrastructure. The AWS cloud supports several disaster recovery architectures, including small customer workload data center failures to rapid failover at scale. Amazon has data centers worldwide, providing disaster recovery services to recover the business IT infrastructure quickly.

15) How to encrypt unencrypted volumes

Answer:

- Create a snapshot of the unencrypted root volume
- Make a copy of the snapshot and select the encrypt option
- Create an AMI from this encrypted snapshot
- Now use this AMI to launch a new instance with encrypted volumes

16) What is AWS EC2 Metadata?

Answer:
EC2 metadata is data about your EC2 instance. Let's see an example to understand how we can use metadata in our cloud formation template script.
View categories of instance metadata from within a running instance using the following IPv4 or IPv6 URIs.

17) What is AWS EC2 userdata?

Answer:

EC2 Userdata is a bootstrap script that gets executed once when the EC2 instance gets launched. Suppose we want to install an apache web server on our Linux instance; we can add the below script in our user data.

```
#! /bin/bash
  sudo su
  sudo yum update
  sudo yum install -y httpd
  sudo chkconfig httpd on
  sudo service httpd start
  echo "<h1>Deployed EC2 With Terraform</h1>" | sudo tee
/var/www/html/index.html
```

18) What are default security features offered as part of your AWS VPC to control traffic towards your application?

Answer:

Here is a list of default security features.

- Security groups - This controls inbound and outgoing traffic at the instance level for EC2 instances, acting as a firewall.
- Network access control lists – They serve as a subnet-level firewall, regulating inbound and outbound traffic.

19) If you would like to check the incoming traffic for your AWS VPC, which logs would you be looking for?

Answer:
VPC Flow Logs: The inbound and outbound traffic from the network interfaces in your VPC is recorded in flow logs

20) What is the difference between Authorization & Authentication in AWS?
Answer:

- **Authentication:** It is how you sign into AWS using your credentials. As a principal, you must be authenticated (signed into AWS) using an entity (root user, IAM user, or IAM role) to send a request to AWS. An IAM user can have long-term credentials such as a username and password or a set of access keys.
- **Authorization:** It is the security process that determines a user or service's level of access. In technology, we use authorization to give users or services permission to access some data or perform a particular action.

21) What is AWS ECS, and what do different types of launch types AWS ECS offer?

Answer:

There are two models that you can use to run your containers:

- **Fargate launch type** - This is a serverless pay-as-you-go option. You can run containers without needing to manage your Infrastructure.
- **EC2 launch type** - Configure and deploy EC2 instances in your cluster to run your containers.

22) What is the key difference between EBS vs. S3 vs EFS?
Answer:

- S3 is object storage, and latency is higher than EBS and EFS; we can host/install OS or application on it
- EBS is block storage, and it is the default storage with an Ec2 instance. We can attach 1 EBS with 1 instance.
- EFS is Elastic File Storage. It is shared storage provided by AWS. We can attach 1 EFS with multiple Ec2 instances.

23) What is AWS Relation Database Service [RDS]? and what are all databases supported by AWS RDS?

Answer:

Amazon is Amazon DAAS (Database as a Service) supports various databases like

1. MSSql(Mysql Server)
2. Oracle
3. Postgres
4. Aurora(serverless and provisioned)
5. Maria DB

24) What is Amazon Aurora Serverless? and how it's different from another managed Aurora Database?
Answer:

It is similar to Aurora Database(MySQL and Postgres compatible). It's an on-demand database. In this database, we don't have to manage/control database instances, and we need not pay the higher compute cost. It assigns compute power as required. In serverless compute capacity denote as ACU(Aurora Capacity unite) we can use mn 1 ACU(2BG RAM) to 256ACU(488GB RAM).

25) What is the Difference between NAT and Internet Gateway?

Answer:

Internet gateways allow AWS resources/instances to connect to public internet on a public subnet, and it provides inbound and outbound traffic on AWS resources. Nat Gateway provides a connection under a private gateway; only inbound traffic is allowed on the NAT gateway.

26) What is Network ACL & Security Group, and what is the difference between them?

Answer:

- Network ACL: NACL stands for Network Access Control Lists. It is a security layer that works on VPC. It controls inbound and outbound internet on one or more subnets.
- Security Group: It acts as a virtual firewall. It controls inbound and outbound traffic in instances
- Difference: Network ACL works on the subnet level, and Security Group works on the Instance/machine level.

27) What is the difference between AWS Cloudwatch default monitoring vs Details Monitoring?

Answer:

In default monitoring, it monitors on a 5-minute span, and it's free; when we enable detailed monitoring, it will start monitoring every 1-minute span. For detailed monitoring, we have to pay for this monitoring.

28) Can a single subnet have more than 1 AZ(Availability Zone) associated with it?

Answer:

No, one subnet means the chunk of IP address, the pool of IP addresses that cannot expand across the availability zone. Multiple subnets can be in a single subnet. For example, there are two subnets, 10.0.1.0 and 10.0.2.0. So, these two subnets can be in EU West one B. But if there is a subnet which is 10.0.1.0, that cannot expand across a single availability zone. It means that it cannot be available within one within us East us West, one B and one A both.

29) What is AWS Route53, and what are its components?

Answer:

AWS Route53 is a DNS service provided by AWS, it's a highly scalable and highly available DNS management system, and it also provides a health-check web service.
AWS route53 components are:

1. DNS management
2. Traffic management
3. Availability monitoring
4. Domain Registration

30) What are the Route53 key features?

Answer:

Route53 key features are:

1. Resolver
2. Traffic flow
3. Latency-based routing
4. Geo DNS
5. Private DNS for Amazon VPC
6. NS Failover
7. Health Checks and Monitoring
8. Domain Registration
9. CloudFront Zone Apex Support
10. S3 Zone Apex Support
11. Amazon ELB Integration
12. Management Console
13. Weighted Round Robin

31) Is terminating and stopping an EC2 instance different processes?

Answer:

No, both are different processes altogether. EC2 performs a regular shutdown when it is stopped. While it is in a stopped state, entire EBS volumes remain associated, so it is possible to start the instance anytime again when you want. When EC2 remains in the stopped state, users don't need to pay for that particular time. Upon EC2 termination, the instance performs a regular shutdown and starts deleting EBS, which is associated with it. To save this kind of unwanted EBS loss, you can stop them from deleting simply by setting the "Delete on Termination" to false. Because the instance gets deleted, it is not possible to run it again in the future.

32) What phases are involved in migrating to AWS Cloud?

Answer:

Migrating applications and data to the AWS cloud involve the following steps:

- Planning Phase: Before starting the migration process, it is important to plan out the migration strategy. This includes identifying the applications and data that will be migrated, assessing their dependencies and requirements, and determining the target environment in AWS.
- Pre-discovery and discovery phase: As part of this phase, the AWS migration specialist from AWS reviews the pre-confirmation application questionnaire as per the line of business. The AWS specialist also conducts interviews with application owners to validate the server inventory by going through a series of discovery-related questions to understand network and storage dependency requirements, high availability/disaster recovery (HA/DR) data points etc.
- Migration path: There are several different approaches to migrating applications and data to AWS, depending on the specific needs and requirements of the applications and data. Some common approaches include
    - Relocate: Containers/VMware Cloud on AWS
    - Rehosting: Lift and shift

    - Replatforming: Lift and reshape
    - Repurchasing: Replace- drop and shop
    - Refactoring: Rewriting or decoupling applications
    - Retain/move
    - Retire/decommission
- Testing & Deployment: After the on-premises applications and data have been migrated, it is important to test them to ensure they function correctly in the AWS environment, which is taken care of by the application migration service, which is part of the AWS Migration hub.

Migrating applications and data to AWS involves careful planning, preparation, and testing to ensure a smooth and successful transition to the cloud.

33) Can you help me know the different types of routing policies offered in AWS Route53?

Answer:

Different types of routing policies in Route53 are:

- **Simple Routing Policy:** When there is only one resource performing the required function for the domain, a basic routing policy, which is a straightforward round-robin strategy, may be used. Based on the values in the resource record set, Route 53 answers DNS queries.
- **Weighted Routing Policy:** Traffic is sent to separate resources according to predetermined weights, such as 75% to one server and 25% to the other, with the aid of a weighted routing policy.
- **Latency-based Routing Policy:** To respond to a DNS query, a latency-based routing policy determines which data center provides us with the least amount of network latency.
- **Failover Routing Policy:** In an active-passive failover arrangement, one resource (the primary) receives all traffic when it is functioning normally, and the other resource (the secondary) receives all traffic when the main is malfunctioning, which is permitted by failover routing rules.
- **Geolocation Routing Policy:** To reply to DNS requests based on the users' geographic locations or the location from which the DNS requests originate, a geolocation routing policy is used.
- **Geoproximity Routing Policy:** Based on the physical locations of the users and the resources, proximity routing assists in directing traffic to those locations.
- **Multivalue Routing Policy:** Multiple values can be returned in answer to DNS requests thanks to multivalue routings, such as the IP addresses of the web servers.

34) Cloud security architect team is planning to limit access to specific services or actions in all of the team's AWS accounts. All accounts belong to a large organization in AWS Organizations. The solution must be scalable, and there must be a single point where permissions can be maintained.

Answer:

Create a service control policy in the root organizational unit to deny access to the services or actions.

Service Control Policy concepts -

- Service Control Policies offer centrally managed access controls for overall IAM entities in targeted accounts. You can use them to make sure to enforce the permissions you want everyone in your business to adhere to. Using Service Control Policies, you can give your proficient developers more freedom to

manage their own permissions because you know they can now only operate within the boundaries you have defined for them.

- You create and apply Service Control Policies through Amazon web services Organizations. When you create an organization, an AWS Organization automatically creates a root first, which forms the parent container for all the accounts in your organization. Inside the root account, you can group accounts in your organization into organizational units (OUs) to simplify the management of these targeted accounts. You can create multiple organizational units within a single organization, and you can create organizational units within other OUs to form a hierarchical structure. You can attach Service Control Policies to the organization's root, organizational units, and individual accounts. Service Control Policies attached to the root and OUs apply to all OUs and accounts inside of them.
- SCPs use the AWS Identity and Access Management (IAM) policy language; however, they do not grant permissions. Service Control Policies enable you to set permission guardrails by defining the maximum available permissions for IAM entities in an account. If a Service Control Policies denies an action for an account, none of the entities in the account can take that action, even if their IAM permissions allow them to do so. The guardrails set in Service Control Policies apply to all
- IAM entities in the account, which include all users, roles, and the account root user.

35) An organization is currently operating a web application backed by an Amazon RDS MySQL database. It has automated backups that are run daily and are not encrypted. A security audit requires future backups to be encrypted and unencrypted backups to be destroyed. The company will make at least one encrypted backup before destroying the old backups. What should be done to enable encryption for future backups?

Answer:

Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot.

However, because you can encrypt a copy of an unencrypted DB snapshot, you can effectively add encryption to an unencrypted DB instance. That is, you can create a snapshot of your DB instance and then create an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot, and thus you have an encrypted copy of your original DB instance.

- DB instances that are encrypted can't be modified to disable encryption.
- You can't have an encrypted read replica of an unencrypted DB instance or an unencrypted read replica of an encrypted DB instance.
- Encrypted read replicas must be encrypted with the same key as the source DB instance when both are in the same AWS Region.
- You can't restore an unencrypted backup or snapshot to an encrypted DB instance.
- To copy an encrypted snapshot from one AWS Region to another, you must specify the KMS key identifier of the destination AWS Region. This is because KMS encryption keys are specific to the AWS Region that they are created.

36) An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%. What should a solutions architect do to maintain the desired performance across all instances in the group?

Answer:

With target-tracking scaling policies, you select a scaling metric and set a target value. Amazon EC2 Autoscaling creates and manages the CloudWatch alarms that trigger the scaling policy and calculates the scaling adjustments based on the metric and the target value. The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value. In addition to keeping the metric close to the target value, a target tracking scaling policy also adjusts to changes in the metric due to a changing load pattern. For example, you can use target tracking scaling to Configure a target tracking scaling policy to keep the average aggregate CPU utilization of your Auto Scaling group at 40 percent. Configure a target tracking scaling policy to keep the request count per target of your Application Load Balancer target group at 1000 for your Autoscaling group.

37) An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%. What should a solutions architect do to maintain the desired performance across all instances in the group?

Answer:

With target-tracking scaling policies, you select a scaling metric and set a target value. Amazon EC2 Autoscaling creates and manages the CloudWatch alarms that trigger the scaling policy and calculates the scaling adjustments based on the metric and the target value. The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value. In addition to keeping the metric close to the target value, a target tracking scaling policy also adjusts to changes in the metric due to a changing load pattern. For example, you can use target tracking scaling to Configure a target tracking scaling policy to keep the average aggregate CPU utilization of your Auto Scaling group at 40 percent. Configure a target tracking scaling policy to keep the request count per target of your Application Load Balancer target group at 1000 for your Autoscaling group.

38) An organization planning to implement an AWS Well-Architected Framework review of an existing workload deployed on AWS. The review identified a public-facing website running on the same Amazon EC2 instance as a Microsoft Active Directory domain controller that was installed recently to support other AWS services. A solutions architect needs to recommend a new design that would improve the security of the architecture and minimize the administrative demand on IT staff. What should the solutions architect recommend?

Answer:

Use AWS Directory Service to create a managed Active Directory. Uninstall Active Directory on the current EC2 instance.
Amazon Web Service Directory lets you run Microsoft Active Directory (AD) as a managed service. Amazon Web Service Directory for Microsoft Active Directory, also referred to as Amazon Web Service Managed Microsoft AD, is powered by Windows

Server 2012 R2. When you target and launch this directory type, it creates a highly available pair of domain controllers connected to your AWS virtual private cloud (VPC). The domain controllers run in different AWS Availability Zones in an AWS region of your choice. Host monitoring and recovery, data replication, snapshots, and software updates are automatically configured and managed for you

39) A company runs an application in a branch office within a small data closet with no virtualized computing resources. The application data is stored on an NFS volume. Compliance standards require a daily offsite backup of the NFS volume. Which solution meets these requirements?

Answer:

Install an Amazon web service Storage Gateway - file gateway hardware appliance on-premises to replicate the data to Amazon S3.

40) A solutions architect is designing storage for a high-performance computing (HPC) environment based on Amazon Linux. The workload stores and processes a large number of engineering drawings that require shared storage and heavy computing.

Answer:

The perfect answer to this use case would be that we should opt for our very new Amazon FSx for Lustre. Amazon FSx for Lustre is a newly launched, fully managed service AWS based on the very well-known Lustre file system.

This AWS Amazon FSx for Lustre provides you with a high-performance filesystem optimized for fast processing of your workloads, such as machine learning[ML], high-performance computing (HPC), video processing, financial modeling, and electronic design automation (EDA), which is very popular nowadays.

AWS Amazon FSx for Lustre allows customers to create a Lustre filesystem on their demand and associate them to an Amazon S3(Simple Storage Service) bucket. As part of this filesystem creation, this Lustre reads the objects in the Amazon S3 buckets and adds that to the file system metadata. Any Lustre client in your AWS virtual private cloud is then able to access data, which gets cached on the high-speed Lustre filesystem. This is an ideal use case for HPC workloads because you can get the speed of an optimized and high-performant Lustre file system without having to manually manage the complexity of its deployments, optimization, and management of the Lustre cluster.

41) What are the different types of pricing models for Amazon EC2?

Answer:

Amazon web services offer multiple options allowing you to choose based on your application or infrastructure needs.

1. **On-Demand EC2 Instances:** Very popularly known as pay-as-you-go, it depends on the Amazon EC2 instance we select, there are no upfront costs, and we only pay for computing capacity per hour or per second.
2. **Spot EC2 Instances:** AWS Spot EC2 Instances can be purchased for up to 90% less than on-demand rates, and these are used to host workloads that are not business-critical.
3. **Reserved EC2 Instances:** Here, we can reserve our instances based on our application or new application implementation roadmaps, where we can save up to 75% on AWS EC2 Reserved Instances when compared to the cost of On-Demand Instances.

4. **Dedicated Hosts:** With a dedicated host option, you purchase a whole physical host from AWS, and this host comes to you on an hourly basis billing manner similar to ec2 times are billed.

42) What are the key benefits of using Amazon Simple Storage Service (S3)?
Answer:
Amazon S3 is one of the most popular and fully managed services by Amazon web service with below outstanding benefits it offers

- Simple data transfer
- Scalability
- Low cost
- Flexibility
- Security
- Availability
- Durability

43) 7) Can we run multiple websites on the EC2 server with one Elastic IP address?
Answer:
We need more than one elastic IP to run multiple websites on the EC2 server, so it's not possible.

44) **Can we speed up data transfer in Snowball? How?**
Answer:
Yes, some specific methods for speeding up Snowball are:

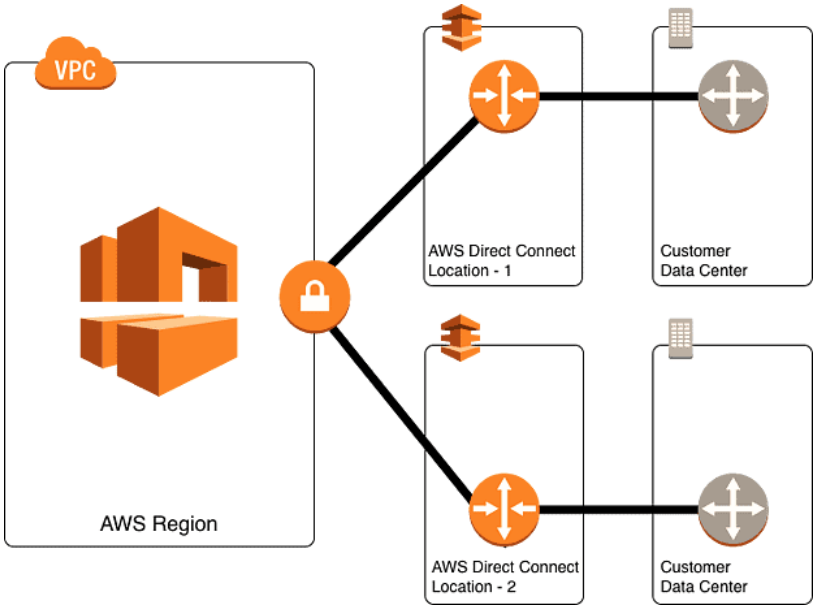
- By simply copying from different hosts to the same Snowball.
- By creating a group of smaller files. This is helpful as it cuts down the encryption issues.

44) Is it possible to run multiple databases on Amazon RDS free of cost?
Answer:
Yes, as per RDS prices, there is an upper limit of 750 hours that on exceeding will be charged. The charge is made only on the extra hours beyond 750.

45) What is a Hypervisor?
Answer:

A Hypervisor is a type of software used to create and run virtual machines. It integrates physical hardware resources into a platform which are distributed virtually to each user.

46) In case AWS Direct Connect fails, will it result in connectivity loss?
Answer:



If a backup of AWS Direct Connect has been configured, it will switch over to the second one in the event of a failure. It is recommended to enable Bidirectional Forwarding Detection (BFD) when configuring your connections to ensure faster detection and failover. On the other hand, if you have configured a backup IPsec VPN connection instead, all VPC traffic will automatically failover to the backup VPN connection. Traffic to/from public resources such as Amazon S3 will be routed over the Internet.

47) How do you handle data archiving in AWS?

Answer:

One way to handle data archiving in AWS is to use Amazon S3 Glacier, which is a secure, durable, and extremely low-cost Amazon S3 storage class for data archiving and long-term backup. With S3 Glacier, you can store data at a cost that is as little as 1/10th of one cent per gigabyte per month.

48) How do you secure an amazon S3 bucket?

Answer:

- To secure an Amazon S3 bucket, you can use a combination of the following measures:
- Access control
- Encryption
- Versioning
- Access logging

49). Can you explain the difference between Amazon EC2 and Amazon Elastic Beanstalk?

Answer:

Amazon EC2 is a web service that provides resizable compute capacity in the cloud, while Amazon Elastic Beanstalk is an easy-to-use service for deploying, running, and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, and Docker.

49) Can you explain the purpose of Amazon Elastic Container Service (ECS)?

Answer:

Amazon Elastic Container Service (ECS) is a fully managed container orchestration service that makes it easy to run, scale, and secure containerized applications on AWS. It allows you to easily run and scale containerized applications using Docker and Amazon Elastic Container Registry (ECR) images.

50) How do you automate the scaling of Amazon EC2 instances?

Answer:

To automate the scaling of Amazon EC2 instances, you can use Amazon Auto Scaling. This service allows you to automatically increase or decrease the number of instances in your Auto Scaling group based on predefined policies and metrics.

51) What is an EIP?

Answer:

EIP (**Elastic IP address**) is a service provided by an EC2 instance. It is basically a static IP address attached to an EC2 instance. This address is associated with your AWS account not with an EC2 instance. You can also disassociate your EIP address from your EC2 instance and map it to another EC2 instance in your AWS account.

Suppose we consider the website www.javatpoint.com points to the instance which has a public IP address. When instance is restarted, then AWS takes another public IP address from the pool and the previous public IP address is no longer valid. Due to this reason, the original link is no longer available between the website and EC2 instance. To overcome from such situation, Elastic IP address or static address is used which does not change.

52)