Top 100+ AWS Interview Questions and Answers for 2023

Lesson 13 of 14By Shyamli Jha

Last updated on Jun 1, 2023141225954

Top 100+ AWS Interview Questions and Answers [Updated]

PreviousNext

Table of Contents

Today's modern world is witnessing a significant change in how businesses and organizations work. Everything is getting digitized, and the introduction of cloud and cloud computing platforms have been a major driving force behind this growth. Today, most businesses are using or are planning to use cloud computing for many of their operations, which consequently has led to a massive surge in the need for cloud professionals.

If you are interested in a career in the cloud industry, your chance has arrived. With cloud computing platforms like AWS taking the present business scenarios by storm, getting trained and certified in that particular platform can provide you with great career prospects.

But in order to get your AWS career started, you need to set up some AWS interviews and ace them. In the spirit of doing that, here are some AWS interview questions and answers that will help you with the interview process. There are a number of different AWS-related questions covered in this article, ranging from basic to advanced, and scenario-based questions as well.

Master AWS, Microsoft Azure and Google Cloud

Post-Graduate Program in Cloud ComputingEXPLORE PROGRAMMaster AWS, Microsoft Azure and Google Cloud

Basic AWS Interview Questions

1. Define and explain the three basic types of cloud services and the AWS products that are built based on them?

The three basic types of cloud services are:

Computing

Storage

Networking

Here are some of the AWS products that are built based on the three cloud service types:

Computing - These include EC2, Elastic Beanstalk, Lambda, Auto-Scaling, and Lightsat.

Storage - These include S3, Glacier, Elastic Block Storage, Elastic File System.

Networking - These include VPC, Amazon CloudFront, Route53

2. What is the relation between the Availability Zone and Region?

AWS regions are separate geographical areas, like the US-West 1 (North California) and Asia South (Mumbai). On the other hand, availability zones are the areas that are present inside the regions. These are generally isolated zones that can replicate themselves whenever required.

aws region

3. What is auto-scaling?

Auto-scaling is a function that allows you to provision and launch new instances whenever there is a demand. It allows you to automatically increase or decrease resource capacity in relation to the demand.

4. What is geo-targeting in CloudFront?

Geo-Targeting is a concept where businesses can show personalized content to their audience based on

their geographic location without changing the URL. This helps you create customized content for the audience of a specific geographical area, keeping their needs in the forefront.

5. What are the steps involved in a CloudFormation Solution?

Here are the steps involved in a CloudFormation solution:

cloud formation

Create or use an existing CloudFormation template using JSON or YAML format.

Save the code in an S3 bucket, which serves as a repository for the code.

Use AWS CloudFormation to call the bucket and create a stack on your template.

CloudFormation reads the file and understands the services that are called, their order, the relationship between the services, and provisions the services one after the other.

6. How do you upgrade or downgrade a system with near-zero downtime?

You can upgrade or downgrade a system with near-zero downtime using the following steps of migration:

Open EC2 console

Choose Operating System AMI

Launch an instance with the new instance type

Install all the updates

Install applications

Test the instance to see if it’s working

If working, deploy the new instance and replace the older instance

Once it’s deployed, you can upgrade or downgrade the system with near-zero downtime.

Take home these interview Q&As and get much more. Download the complete AWS Interview Guide here:

7. What are the tools and techniques that you can use in AWS to identify if you are paying more than you should be, and how to correct it?

You can know that you are paying the correct amount for the resources that you are using by employing the following resources:

Check the Top Services Table

It is a dashboard in the cost management console that shows you the top five most used services. This will let you know how much money you are spending on the resources in question.

Cost Explorer

There are cost explorer services available that will help you to view and analyze your usage costs for the last 13 months. You can also get a cost forecast for the upcoming three months.

AWS Budgets

This allows you to plan a budget for the services. Also, it will enable you to check if the current plan meets your budget and the details of how you use the services.

Cost Allocation Tags

This helps in identifying the resource that has cost more in a particular month. It lets you organize your resources and cost allocation tags to keep track of your AWS costs.

What Do Tech Companies Want in Cloud Experts?

Post-Graduate Program in Cloud ComputingEXPLORE PROGRAMWhat Do Tech Companies Want in Cloud Experts?

8. Is there any other alternative tool to log into the cloud environment other than console?

The that can help you log into the AWS resources are:

Putty

AWS CLI for Linux

AWS CLI for Windows

AWS CLI for Windows CMD

AWS SDK

Eclipse

9. What services can be used to create a centralized logging solution?

The essential services that you can use are Amazon CloudWatch Logs, store them in Amazon S3, and then use Amazon Elastic Search to visualize them. You can use Amazon Kinesis Firehose to move the data from Amazon S3 to Amazon ElasticSearch.

centralized logging

10. What are the native AWS Security logging capabilities?

Most of the AWS services have their logging options. Also, some of them have an account level logging, like in AWS CloudTrail, AWS Config, and others. Let's take a look at two services in specific:

AWS CloudTrail

This is a service that provides a history of the AWS API calls for every account. It lets you perform security analysis, resource change tracking, and compliance auditing of your AWS environment as well. The best part about this service is that it enables you to configure it to send notifications via AWS SNS when new logs are delivered.

AWS Config

This helps you understand the configuration changes that happen in your environment. This service provides an AWS inventory that includes configuration history, configuration change notification, and relationships between AWS resources. It can also be configured to send information via AWS SNS when new logs are delivered.

11. What is a DDoS attack, and what services can minimize them?

DDoS is a cyber-attack in which the perpetrator accesses a website and creates multiple sessions so that the other legitimate users cannot access the service. The native tools that can help you deny the DDoS attacks on your AWS services are:

AWS Shield

AWS WAF

Amazon Route53

Amazon CloudFront

ELB

VPC

DDOS attack

12. You are trying to provide a service in a particular region, but you do not see the service in that region. Why is this happening, and how do you fix it?

Not all Amazon AWS services are available in all regions. When Amazon initially launches a new service, it doesn't get immediately published in all the regions. They start small and then slowly expand to other regions. So, if you don't see a specific service in your region, chances are the service hasn't been published in your region yet. However, if you want to get the service that is not available, you can switch to the nearest region that provides the services.

13. How do you set up a system to monitor website metrics in real-time in AWS?

Amazon CloudWatch helps you to monitor the application status of various AWS services and custom events. It helps you to monitor:

State changes in Amazon EC2

Auto-scaling lifecycle events

Scheduled events

AWS API calls

Console sign-in events

amazon cloud watch

14. What are the different types of virtualization in AWS, and what are the differences between them?

The three major types of virtualization in AWS are:

Hardware Virtual Machine (HVM)

It is a fully virtualized hardware, where all the virtual machines act separate from each other. These virtual machines boot by executing a master boot record in the root block device of your image.

Paravirtualization (PV)

Paravirtualization-GRUB is the bootloader that boots the PV AMIs. The PV-GRUB chain loads the kernel specified in the menu.

Paravirtualization on HVM

PV on HVM helps operating systems take advantage of storage and network I/O available through the host.

15. Name some of the AWS services that are not region-specific

AWS services that are not region-specific are:

IAM

Route 53

Web Application Firewall

CloudFront

Get Certified in AWS, Azure and Google Cloud

Post-Graduate Program in Cloud ComputingEXPLORE PROGRAMGet Certified in AWS, Azure and Google Cloud

16. What are the differences between NAT Gateways and NAT Instances?

While both NAT Gateways and NAT Instances serve the same function, they still have some key differences.

Differences

17. What is CloudWatch?

The Amazon CloudWatch has the following features:

Depending on multiple metrics, it participates in triggering alarms.

Helps in monitoring the AWS environments like CPU utilization, EC2, Amazon RDS instances, Amazon SQS, S3, Load Balancer, SNS, etc.

18. What is an Elastic Transcoder?

To support multiple devices with various resolutions like laptops, tablets, and smartphones, we need to change the resolution and format of the video. This can be done easily by an AWS Service tool called the Elastic Transcoder, which is a media transcoding in the cloud that exactly lets us do the needful. It is easy to use, cost-effective, and highly scalable for businesses and developers.

AWS Interview Questions for Intermediate and Experienced

19. With specified private IP addresses, can an Amazon Elastic Compute Cloud (EC2) instance be launched? If so, which Amazon service makes it possible?

Yes. Utilizing VPC makes it possible (Virtual Private Cloud).

20. Define Amazon EC2 regions and availability zones?

Availability zones are geographically separate locations. As a result, failure in one zone has no effect on EC2 instances in other zones. When it comes to regions, they may have one or more availability zones. This configuration also helps to reduce latency and costs.

21. Explain Amazon EC2 root device volume?

The image that will be used to boot an EC2 instance is stored on the root device drive. This occurs when an Amazon AMI runs a new EC2 instance. And this root device volume is supported by EBS or an instance store. In general, the root device data on Amazon EBS is not affected by the lifespan of an EC2 instance.

22. Mention the different types of instances in Amazon EC2 and explain its features.

General Purpose Instances: They are used to compute a range of workloads and aid in the allocation of processing, memory, and networking resources.

Compute Optimized Instances: These are ideal for compute-intensive applications. They can handle batch processing workloads, high-performance web servers, machine learning inference, and various other tasks.

Memory Optimized: They process workloads that handle massive datasets in memory and deliver them quickly.

Accelerated Computing: It aids in the execution of floating-point number calculations, data pattern matching, and graphics processing. These functions are carried out using hardware accelerators.

Storage Optimised: They handle tasks that require sequential read and write access to big data sets on local storage.

23. Will your standby RDS be launched in the same availability zone as your primary?

No, standby instances are launched in different availability zones than the primary, resulting in physically separate infrastructures. This is because the entire purpose of standby instances is to prevent infrastructure failure. As a result, if the primary instance fails, the backup instance will assist in recovering all of the data.

Advanced AWS Interview Questions and Answers

24. What is the difference between a Spot Instance, an On-demand Instance, and a Reserved Instance?

Spot instances are unused EC2 instances that users can use at a reduced cost.

When you use on-demand instances, you must pay for computing resources without making long-term obligations.

Reserved instances, on the other hand, allow you to specify attributes such as instance type, platform, tenancy, region, and availability zone. Reserved instances offer significant reductions and capacity reservations when instances in certain availability zones are used.

25. How would you address a situation in which the relational database engine frequently collapses when traffic to your RDS instances increases, given that the RDS instance replica is not promoted as the master instance?

A larger RDS instance type is required for handling significant quantities of traffic, as well as producing manual or automated snapshots to recover data if the RDS instance fails.

26. What do you understand by 'changing' in Amazon EC2?

To make limit administration easier for customers, Amazon EC2 now offers the option to switch from the current 'instance count-based limitations' to the new 'vCPU Based restrictions.' As a result, when launching a combination of instance types based on demand, utilization is measured in terms of the number of vCPUs.

27. Define Snapshots in Amazon Lightsail?

The point-in-time backups of EC2 instances, block storage drives, and databases are known as snapshots. They can be produced manually or automatically at any moment. Your resources can always be restored using snapshots, even after they have been created. These resources will also perform the same tasks as the original ones from which the snapshots were made.

AWS Scenario-based Questions

28. On an EC2 instance, an application of yours is active. Once the CPU usage on your instance hits 80%, you must reduce the load on it. What strategy do you use to complete the task?

It can be accomplished by setting up an autoscaling group to deploy additional instances, when an EC2 instance's CPU use surpasses 80% and by allocating traffic across instances via the creation of an application load balancer and the designation of EC2 instances as target instances.

29. Multiple Linux Amazon EC2 instances running a web application for a firm are being used, and data is being stored on Amazon EBS volumes. The business is searching for a way to provide storage that complies with atomicity, consistency, isolation, and durability while also increasing the application's resilience in the event of a breakdown (ACID). What steps should a solutions architect take to fulfill these demands?

AWS Auto Scaling groups can create an application load balancer that spans many availability zones.

Mount a target on each instance and save data on Amazon EFS.

30. Your business prefers to use its email address and domain to send and receive compliance emails. What service do you recommend to implement it easily and budget-friendly?

This can be accomplished by using Amazon Simple Email Service (Amazon SES), a cloud-based email-sending service.

Technical and Non-Technical AWS Interview Questions

31. Describe SES.

Amazon offers the Simple Email Service (SES) service, which allows you to send bulk emails to customers swiftly at a minimal cost.

32. Describe PaaS.

PaaS supports the operation of multiple cloud platforms, primarily for the development, testing, and oversight of the operation of the program.

33. How many S3 buckets can be created?

Up to 100 buckets can be created by default.

34. What is the maximum limit of elastic IPs anyone can produce?

A maximum of five elastic IP addresses can be generated per location and AWS account.

AWS Questions for Amazon EC2

35. What is Amazon EC2?

EC2 is short for Elastic Compute Cloud, and it provides scalable computing capacity. Using Amazon EC2 eliminates the need to invest in hardware, leading to faster development and deployment of applications. You can use Amazon EC2 to launch as many or as few virtual servers as needed, configure security and networking, and manage storage. It can scale up or down to handle changes in requirements, reducing the need to forecast traffic. EC2 provides virtual computing environments called

“instances.”

36. What Are Some of the Security Best Practices for Amazon EC2?

Security best practices for Amazon EC2 include using Identity and Access Management (IAM) to control access to AWS resources; restricting access by only allowing trusted hosts or networks to access ports on an instance; only opening up those permissions you require, and disabling password-based logins for instances launched from your AMI.

37. Can S3 Be Used with EC2 Instances, and If Yes, How?

Amazon S3 can be used for instances with root devices backed by local instance storage. That way, developers have access to the same highly scalable, reliable, fast, inexpensive data storage infrastructure that Amazon uses to run its own global network of websites. To execute systems in the Amazon EC2 environment, developers load Amazon Machine Images (AMIs) into Amazon S3 and then move them between Amazon S3 and Amazon EC2.

Amazon EC2 and Amazon S3 are two of the best-known web services that make up AWS.

38. What is the difference between stopping and terminating an EC2 instance?

While you may think that both stopping and terminating are the same, there is a difference. When you stop an EC2 instance, it performs a normal shutdown on the instance and moves to a stopped state. However, when you terminate the instance, it is transferred to a stopped state, and the EBS volumes attached to it are deleted and can never be recovered.

39. What are the different types of EC2 instances based on their costs?

The three types of EC2 instances are:

On-demand Instance

It is cheap for a short time but not when taken for the long term

Spot Instance

It is less expensive than the on-demand instance and can be bought through bidding.

Reserved Instance

If you are planning to use an instance for a year or more, then this is the right one for you.

Want a Job at AWS? Find Out What It Takes

Cloud Architect Master's ProgramEXPLORE PROGRAMWant a Job at AWS? Find Out What It Takes

40. How do you set up SSH agent forwarding so that you do not have to copy the key every time you log in?

Here's how you accomplish this:

Go to your PuTTY Configuration

Go to the category SSH -> Auth

Enable SSH agent forwarding to your instance

Putty configuration

41. What are Solaris and AIX operating systems? Are they available with AWS?

Solaris is an operating system that uses SPARC processor architecture, which is not supported by the public cloud currently.

AIX is an operating system that runs only on Power CPU and not on Intel, which means that you cannot create AIX instances in EC2.

Since both the operating systems have their limitations, they are not currently available with AWS.

42. How do you configure CloudWatch to recover an EC2 instance?

Here's how you can configure them:

Create an Alarm using Amazon CloudWatch

In the Alarm, go to Define Alarm -> Actions tab

Choose Recover this instance option

create alarm

43. What are the common types of AMI designs?

There are many types of AMIs, but some of the common AMIs are:

Fully Baked AMI

Just Enough Baked AMI (JeOS AMI)

Hybrid AMI

44. What are Key-Pairs in AWS?

The Key-Pairs are password-protected login credentials for the Virtual Machines that are used to prove our identity while connecting the Amazon EC2 instances. The Key-Pairs are made up of a Private Key and a Public Key which lets us connect to the instances.

AWS Interview Questions for S3

45. What is Amazon S3?

S3 is short for Simple Storage Service, and Amazon S3 is the most supported storage platform available. S3 is object storage that can store and retrieve any amount of data from anywhere. Despite that versatility, it is practically unlimited as well as cost-effective because it is storage available on demand. In addition to these benefits, it offers unprecedented levels of durability and availability. Amazon S3 helps to manage data for cost optimization, access control, and compliance.

46. How can you recover/login to an EC2 instance for which you have lost the key?

Follow the steps provided below to recover an EC2 instance if you have lost the key:

Verify that the EC2Config service is running

Detach the root volume for the instance

Attach the volume to a temporary instance

Modify the configuration file

Restart the original instance

47. What are some critical differences between AWS S3 and EBS?

Here are some differences between AWS S3 and EBS

feature differences

48. How do you allow a user to gain access to a specific bucket?

You need to follow the four steps provided below to allow access. They are:

Categorize your instances

Define how authorized users can manage specific servers.

Lockdown your tags

Attach your policies to IAM users

49. How can you monitor S3 cross-region replication to ensure consistency without actually checking the bucket?

Follow the flow diagram provided below to monitor S3 cross-region replication:

S3 cross region

50. What is SnowBall?

To transfer terabytes of data outside and inside of the AWS environment, a small application called SnowBall is used.

Data transferring using SnowBall is done in the following ways:

A job is created.

The SnowBall application is connected.

The data is copied into the SnowBall application.

Data is then moved to the AWS S3.

51. What are the Storage Classes available in Amazon S3?

The Storage Classes that are available in the Amazon S3 are the following:

Amazon S3 Glacier Instant Retrieval storage class

Amazon S3 Glacier Flexible Retrieval (Formerly S3 Glacier) storage class

Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive)

S3 Outposts storage class

Amazon S3 Standard-Infrequent Access (S3 Standard-IA)

Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Amazon S3 Standard (S3 Standard)

Amazon S3 Reduced Redundancy Storage

Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)

AWS Interview Questions for VPC

52. What Is Amazon Virtual Private Cloud (VPC) and Why Is It Used?

A VPC is the best way of connecting to your cloud resources from your own data center. Once you

connect your datacenter to the VPC in which your instances are present, each instance is assigned a private IP address that can be accessed from your data center. That way, you can access your public cloud resources as if they were on your own private network.

53. VPC is not resolving the server through DNS. What might be the issue, and how can you fix it?

To fix this problem, you need to enable the DNS hostname resolution, so that the problem resolves itself.

54. How do you connect multiple sites to a VPC?

If you have multiple VPN connections, you can provide secure communication between sites using the AWS VPN CloudHub. Here's a diagram that will show you how to connect various sites to a VPC:

customer gateway

55. Name and explain some security products and features available in VPC?

Here is a selection of security products and features:

Security groups - This acts as a firewall for the EC2 instances, controlling inbound and outbound traffic at the instance level.

Network access control lists - It acts as a firewall for the subnets, controlling inbound and outbound traffic at the subnet level.

Flow logs - These capture the inbound and outbound traffic from the network interfaces in your VPC.

56. How do you monitor Amazon VPC?

You can monitor VPC by using:

CloudWatch and CloudWatch logs

VPC Flow Logs

57. How many Subnets can you have per VPC?

We can have up to 200 Subnets per Amazon Virtual Private Cloud (VPC).

General AWS Interview Questions

58. When Would You Prefer Provisioned IOPS over Standard Rds Storage?

You would use Provisioned IOPS when you have batch-oriented workloads. Provisioned IOPS delivers high IO rates, but it is also expensive. However, batch processing workloads do not require manual intervention.

59. How Do Amazon Rds, Dynamodb, and Redshift Differ from Each Other?

Amazon RDS is a database management service for relational databases. It manages patching, upgrading, and data backups automatically. It's a database management service for structured data only. On the other hand, DynamoDB is a NoSQL database service for dealing with unstructured data. Redshift is a data warehouse product used in data analysis.

60. What Are the Benefits of AWS's Disaster Recovery?

Businesses use cloud computing in part to enable faster disaster recovery of critical IT systems without the cost of a second physical site. The AWS cloud supports many popular disaster recovery architectures ranging from small customer workload data center failures to environments that enable rapid failover at scale. With data centers all over the world, AWS provides a set of cloud-based disaster recovery services that enable rapid recovery of your IT infrastructure and data.

61. How can you add an existing instance to a new Auto Scaling group?

Here's how you can add an existing instance to a new Auto Scaling group:

Open EC2 console

Select your instance under Instances

Choose Actions -> Instance Settings -> Attach to Auto Scaling Group

Select a new Auto Scaling group

Attach this group to the Instance

Edit the Instance if needed

Once done, you can successfully add the instance to a new Auto Scaling group

Transform Yourself into a Cloud Architect

Cloud Architect Master's ProgramEXPLORE PROGRAMTransform Yourself into a Cloud Architect

62. What are the factors to consider while migrating to Amazon Web Services?

Here are the factors to consider during AWS migration:

Operational Costs - These include the cost of infrastructure, ability to match demand and supply, transparency, and others.

Workforce Productivity

Cost avoidance

Operational resilience

Business agility

63. What is RTO and RPO in AWS?

RTO or Recovery Time Objective is the maximum time your business or organization is willing to wait for a recovery to complete in the wake of an outage. On the other hand, RPO or Recovery Point Objective is the maximum amount of data loss your company is willing to accept as measured in time.

64. If you would like to transfer vast amounts of data, which is the best option among Snowball, Snowball Edge, and Snowmobile?

AWS Snowball is basically a data transport solution for moving high volumes of data into and out of a specified AWS region. On the other hand, AWS Snowball Edge adds additional computing functions apart from providing a data transport solution. The snowmobile is an exabyte-scale migration service that allows you to transfer data up to 100 PB.

65. Explain what T2 instances are?

The T2 Instances are intended to give the ability to burst to a higher performance whenever the workload demands it and also provide a moderate baseline performance to the CPU.

The T2 instances are General Purpose instance types and are low in cost as well. They are usually used wherever workloads do not consistently or often use the CPU.

66. What are the advantages of AWS IAM?

AWS IAM allows an administrator to provide multiple users and groups with granular access. Various user groups and users may require varying levels of access to the various resources that have been developed. We may assign roles to users and create roles with defined access levels using IAM.

It further gives us Federated Access, which allows us to grant applications and users access to resources without having to create IAM Roles.

67. Explain Connection Draining

Connection Draining is an AWS service that allows us to serve current requests on the servers that are either being decommissioned or updated.

By enabling this Connection Draining, we let the Load Balancer make an outgoing instance finish its existing requests for a set length of time before sending it any new requests. A departing instance will immediately go off if Connection Draining is not enabled, and all pending requests will fail.

68. What is Power User Access in AWS?

The AWS Resources owner is identical to an Administrator User. The Administrator User can build, change, delete, and inspect resources, as well as grant permissions to other AWS users.

Administrator Access without the ability to control users and permissions is provided to a Power User. A Power User Access user cannot provide permissions to other users but has the ability to modify, remove, view, and create resources.

AWS Questions for CloudFormation

69. How is AWS CloudFormation different from AWS Elastic Beanstalk?

Here are some differences between AWS CloudFormation and AWS Elastic Beanstalk:

AWS CloudFormation helps you provision and describe all of the infrastructure resources that are present in your cloud environment. On the other hand, AWS Elastic Beanstalk provides an environment that makes it easy to deploy and run applications in the cloud.

AWS CloudFormation supports the infrastructure needs of various types of applications, like legacy applications and existing enterprise applications. On the other hand, AWS Elastic Beanstalk is combined with the developer tools to help you manage the lifecycle of your applications.

70. What are the elements of an AWS CloudFormation template?

AWS CloudFormation templates are YAML or JSON formatted text files that are comprised of five essential elements, they are:

Template parameters

Output values

Data tables

Resources

File format version

71. What happens when one of the resources in a stack cannot be created successfully?

If the resource in the stack cannot be created, then the CloudFormation automatically rolls back and terminates all the resources that were created in the CloudFormation template. This is a handy feature when you accidentally exceed your limit of Elastic IP addresses or don't have access to an EC2 AMI.

AWS cloud formation

AWS Questions for Elastic Block Storage

72. How can you automate EC2 backup using EBS?

Use the following steps in order to automate EC2 backup using EBS:

Get the list of instances and connect to AWS through API to list the Amazon EBS volumes that are attached locally to the instance.

List the snapshots of each volume, and assign a retention period of the snapshot. Later on, create a snapshot of each volume.

Make sure to remove the snapshot if it is older than the retention period.

73. What is the difference between EBS and Instance Store?

EBS is a kind of permanent storage in which the data can be restored at a later point. When you save data in the EBS, it stays even after the lifetime of the EC2 instance. On the other hand, Instance Store is temporary storage that is physically attached to a host machine. With an Instance Store, you cannot detach one instance and attach it to another. Unlike in EBS, data in an Instance Store is lost if any instance is stopped or terminated.

74. Can you take a backup of EFS like EBS, and if yes, how?

Yes, you can use the EFS-to-EFS backup solution to recover from unintended changes or deletion in Amazon EFS. Follow these steps:

Sign in to the AWS Management Console

Click the launch EFS-to-EFS-restore button

Use the region selector in the console navigation bar to select region

Verify if you have chosen the right template on the Select Template page

Assign a name to your solution stack

Review the parameters for the template and modify them if necessary

75. How do you auto-delete old snapshots?

Here’s the procedure for auto-deleting old snapshots:

As per procedure and best practices, take snapshots of the EBS volumes on Amazon S3.

Use AWS Ops Automator to handle all the snapshots automatically.

This allows you to create, copy, and delete Amazon EBS snapshots.

S3

AWS Interview Questions for Elastic Load Balancing

76. What are the different types of load balancers in AWS?

There are three types of load balancers that are supported by Elastic Load Balancing:

Application Load Balancer

Network Load Balancer

Classic Load Balancer

77. What are the different uses of the various load balancers in AWS Elastic Load Balancing?

Application Load Balancer

Used if you need flexible application management and TLS termination.

Network Load Balancer

Used if you require extreme performance and static IPs for your applications.

Classic Load Balancer

Used if your application is built within the EC2 Classic network

AWS Interview Questions for Security

78. What Is Identity and Access Management (IAM) and How Is It Used?

Identity and Access Management (IAM) is a web service for securely controlling access to AWS services. IAM lets you manage users, security credentials such as access keys, and permissions that control which AWS resources users and applications can access.

79. How can you use AWS WAF in monitoring your AWS applications?

AWS WAF or AWS Web Application Firewall protects your web applications from web exploitations. It helps you control the traffic flow to your applications. With WAF, you can also create custom rules that block common attack patterns. It can be used for three cases: allow all requests, prevent all requests,

and count all requests for a new policy.

80. What are the different AWS IAM categories that you can control?

Using AWS IAM, you can do the following:

Create and manage IAM users

Create and manage IAM groups

Manage the security credentials of the users

Create and manage policies to grant access to AWS services and resources

81. What are the policies that you can set for your users' passwords?

Here are some of the policies that you can set:

You can set a minimum length of the password, or you can ask the users to add at least one number or special characters in it.

You can assign requirements of particular character types, including uppercase letters, lowercase letters, numbers, and non-alphanumeric characters.

You can enforce automatic password expiration, prevent reuse of old passwords, and request for a password reset upon their next AWS sign in.

You can have the AWS users contact an account administrator when the user has allowed the password to expire.

82. What is the difference between an IAM role and an IAM user?

The two key differences between the IAM role and IAM user are:

An IAM role is an IAM entity that defines a set of permissions for making AWS service requests, while an IAM user has permanent long-term credentials and is used to interact with the AWS services directly.

In the IAM role, trusted entities, like IAM users, applications, or an AWS service, assume roles whereas the IAM user has full access to all the AWS IAM functionalities.

83. What are the managed policies in AWS IAM?

There are two types of managed policies; one that is managed by you and one that is managed by AWS. They are IAM resources that express permissions using IAM policy language. You can create, edit, and manage them separately from the IAM users, groups, and roles to which they are attached.

84. Can you give an example of an IAM policy and a policy summary?

Here's an example of an IAM policy to grant access to add, update, and delete objects from a specific folder.

IAM policy

Here's an example of a policy summary:

policy summary

85. How does AWS IAM help your business?

IAM enables to:

Manage IAM users and their access - AWS IAM provides secure resource access to multiple users

Manage access for federated users – AWS allows you to provide secure access to resources in your AWS account to your employees and applications without creating IAM roles

AWS Interview Questions for Route 53

86. What Is Amazon Route 53?

Amazon Route 53 is a scalable and highly available Domain Name System (DNS). The name refers to TCP or UDP port 53, where DNS server requests are addressed.

87. What Is Cloudtrail and How Do Cloudtrail and Route 53 Work Together?

CloudTrail is a service that captures information about every request sent to the Amazon Route 53 API by an AWS account, including requests that are sent by IAM users. CloudTrail saves log files of these

requests to an Amazon S3 bucket. CloudTrail captures information about all requests. You can use information in the CloudTrail log files to determine which requests were sent to Amazon Route 53, the IP address that the request was sent from, who sent the request, when it was sent, and more.

88. What is the difference between Latency Based Routing and Geo DNS?

The Geo Based DNS routing takes decisions based on the geographic location of the request. Whereas, the Latency Based Routing utilizes latency measurements between networks and AWS data centers. Latency Based Routing is used when you want to give your customers the lowest latency possible. On the other hand, Geo Based routing is used when you want to direct the customer to different websites based on the country or region they are browsing from.

89. What is the difference between a Domain and a Hosted Zone?

Domain

A domain is a collection of data describing a self-contained administrative and technical unit. For example, www.simplilearn.com is a domain and a general DNS concept.

Hosted zone

A hosted zone is a container that holds information about how you want to route traffic on the internet for a specific domain. For example, lms.simplilearn.com is a hosted zone.

90. How does Amazon Route 53 provide high availability and low latency?

Here’s how Amazon Route 53 provides the resources in question:

Globally Distributed Servers

Amazon is a global service and consequently has DNS services globally. Any customer creating a query from any part of the world gets to reach a DNS server local to them that provides low latency.

Dependency

Route 53 provides a high level of dependability required by critical applications

Optimal Locations

Route 53 uses a global anycast network to answer queries from the optimal position automatically.

AWS Interview Questions for Config

91. How does AWS config work with AWS CloudTrail?

AWS CloudTrail records user API activity on your account and allows you to access information about the activity. Using CloudTrail, you can get full details about API actions such as the identity of the caller, time of the call, request parameters, and response elements. On the other hand, AWS Config records point-in-time configuration details for your AWS resources as Configuration Items (CIs).

You can use a CI to ascertain what your AWS resource looks like at any given point in time. Whereas, by using CloudTrail, you can quickly answer who made an API call to modify the resource. You can also use Cloud Trail to detect if a security group was incorrectly configured.

92. Can AWS Config aggregate data across different AWS accounts?

Yes, you can set up AWS Config to deliver configuration updates from different accounts to one S3 bucket, once the appropriate IAM policies are applied to the S3 bucket.

AWS Interview Questions for Database

93. How are reserved instances different from on-demand DB instances?

Reserved instances and on-demand instances are the same when it comes to function. They only differ in how they are billed.

Reserved instances are purchased as one-year or three-year reservations, and in return, you get very low hourly based pricing when compared to the on-demand cases that are billed on an hourly basis.

94. Which type of scaling would you recommend for RDS and why?

There are two types of scaling - vertical scaling and horizontal scaling. Vertical scaling lets you vertically

scale up your master database with the press of a button. A database can only be scaled vertically, and there are 18 different instances in which you can resize the RDS. On the other hand, horizontal scaling is good for replicas. These are read-only replicas that can only be done through Amazon Aurora.

95. What is a maintenance window in Amazon RDS? Will your DB instance be available during maintenance events?

RDS maintenance window lets you decide when DB instance modifications, database engine version upgrades, and software patching have to occur. The automatic scheduling is done only for patches that are related to security and durability. By default, there is a 30-minute value assigned as the maintenance window and the DB instance will still be available during these events though you might observe a minimal effect on performance.

96. What are the consistency models in DynamoDB?

There are two consistency models In DynamoDB. First, there is the Eventual Consistency Model, which maximizes your read throughput. However, it might not reflect the results of a recently completed write. Fortunately, all the copies of data usually reach consistency within a second. The second model is called the Strong Consistency Model. This model has a delay in writing the data, but it guarantees that you will always see the updated data every time you read it.

97. What type of query functionality does DynamoDB support?

DynamoDB supports GET/PUT operations by using a user-defined primary key. It provides flexible querying by letting you query on non-primary vital attributes using global secondary indexes and local secondary indexes.

1. What is AWS?

AWS (Amazon Web Services) is a platform to provide secure cloud services, database storage, offerings to compute power, content delivery, and other services to help business level and develop.

Want to learn the basics of AWS Cloud Solutions? Check out our AWS Certification Course!

2. Give the comparison between AWS and OpenStack.

Criteria AWS OpenStack

License Amazon proprietary Open-source

Operating system Provided as per the cloud administrator AMIs provided by AWS

Performing repeatable operations Through templates Through text files

3. What is the importance of buffer in Amazon Web Services?

An Elastic Load Balancer ensures that the incoming traffic is distributed optimally across various AWS instances. A buffer will synchronize different components and makes the arrangement additionally elastic to a burst of load or traffic. The components are prone to work in an unstable way of receiving and processing requests. The buffer creates an equilibrium linking various apparatus and crafts them to work at an identical rate to supply more rapid services.

4. How are Spot Instance, On-demand Instance, and Reserved Instance different from one another?

Both Spot Instance and On-demand Instance are models for pricing.

Spot Instance On-demand Instance

With Spot Instance, customers can purchase compute capacity with no upfront commitment at all. With On-demand Instance, users can launch instances at any time based on the demand.

Spot Instances are spare Amazon instances that you can bid for. On-demand Instances are suitable for the high-availability needs of applications.

When the bidding price exceeds the spot price, the instance is automatically launched, and the spot price fluctuates based on supply and demand for instances. On-demand Instances are launched by users only with the pay-as-you-go model.

When the bidding price is less than the spot price, the instance is immediately taken away by Amazon. On-demand Instances will remain persistent without any automatic termination from Amazon.

Spot Instances are charged on an hourly basis. On-demand Instances are charged on a per-second basis

5. Why do we make subnets?

Creating subnets means dividing a large network into smaller ones. These subnets can be created for several reasons. For example, creating and using subnets can help reduce congestion by making sure that the traffic destined for a subnet stays in that subnet. This helps in efficiently routing the traffic coming to the network that reduces the network's load.

Learn more about AWS from this AWS Training in New York to get ahead in your career!

6. Is there a way to upload a file that is greater than 100 megabytes in Amazon S3?

Yes, it is possible by using the multipart upload utility from AWS. With the multipart upload utility, larger files can be uploaded in multiple parts that are uploaded independently. You can also decrease upload time by uploading these parts in parallel. After the upload is done, the parts will be merged into a single object or file to create the original file from which the parts were created.

To learn more about the Amazon S3 bucket, read the blog.

7. What is the maximum number of S3 buckets you can create?

The maximum number of S3 buckets that can be created is 100.

8. How can you save the data on root volume on an EBS-backed machine?

We can save the data by overriding the terminate option

9. When should you use the classic load balancer and the application load balancer?

The classic load balancer is used for simple load balancing of traffic across multiple EC2 instances.

Classic Load Balancer

While, the application load balancing is used for more intelligent load balancing, based on the multi-tier architecture or container-based architecture of the application. Application load balancing is mostly used when there is a need to route traffic to multiple services.

Classic Load Balancer

Want to learn about AWS DevOps! Check out our blog on What is AWS DevOps.

10. How many total VPCs per account/region and subnets per VPC can you have?

We can have a total of 5 VPCs for every account/region and 200 subnets for every VPC that you have.

11. Your organization has decided to have all their workload on the public cloud. But, due to certain security concerns, your organization decides to distribute some of the workload on private servers. You are asked to suggest a cloud architecture for your organization. What will be your suggestion?

A hybrid cloud. The hybrid cloud architecture is where an organization can use the public cloud for shared resources and the private cloud for its confidential workloads.

Career Transition

12. Which one of the storage solutions offered by AWS would you use if you need extremely low pricing and data archiving?

AWS Glacier is an extremely low-cost storage service offered by Amazon that is used for data archiving and backup purposes. The longer you store data in Glacier, the lesser it will cost you.

Go through the AWS Course in London to get a clear understanding of AWS!

13. You have connected four instances to ELB. To automatically terminate your unhealthy instances and replace them with new ones, which functionality would you use?

Auto-scaling groups

14. The data on the root volumes of store-backed and EBS-backed instances get deleted by default when they are terminated. If you want to prevent that from happening, which instance would you use?

EBS-backed instances. EBS-backed instances use EBS volume as their root volume. EBS volume consists of virtual drives that can be easily backed up and duplicated by snapshots.

EBS Backed Instances

The biggest advantage of EBS-backed volumes is that the data can be configured to be stored for later retrieval even if the virtual machine or the instances are shut down.

15. How will you configure an Amazon S3 bucket to serve static assets for your public web application?

By configuring the bucket policy to provide public read access to all objects

That is all we have in our section on basic Amazon Web Services interview questions section. Let's move onto the next section on AWS interview questions for experienced professionals.

Intermediate AWS Interview Questions

16. Your organization wants to send and receive compliance emails to its clients using its own email address and domain. What service would you suggest for achieving the same in an easy and cost-effective way?

Amazon Simple Email Service (Amazon SES), which is a cloud-based email sending service, can be used for this purpose.

17. Can you launch Amazon Elastic Compute Cloud (EC2) instances with predetermined private IP addresses? If yes, then with which Amazon service it is possible?

Yes. It is possible by using VPC (Virtual Private Cloud).

18. If you launched a standby RDS, will it be launched in the same availability zone as your primary?

No, standby instances are automatically launched in different availability zones than the primary, making them physically independent infrastructures. This is because the whole purpose of standby instances is to prevent infrastructure failure. So, in case the primary goes down, the standby instance will help recover all of the data.

19. What is the name of Amazon's Content Delivery Network ?

Amazon CloudFront

20. Which Amazon solution will you use if you want to accelerate moving petabytes of data in and out of AWS, using storage devices that are designed to be secure for data transfer?

Amazon Snowball. AWS Snowball is the data transport solution for large amounts of data that need to be moved into and out of AWS using physical storage devices.

21. If you are running your DB instance as Multi-AZ deployment, can you use standby DB instances along with your primary DB instance?

No, the standby DB instance cannot be used along with the primary DB instances since the standby DB instances are supposed to be used only if the primary instance goes down.

22. Your organization is developing a new multi-tier web application in AWS. Being a fairly new and small organization, there’s limited staff. But, the organization requires high availability. This new application comprises complex queries and table joins. Which Amazon service will be the best solution for your organization’s requirements?

DynamoDB will be the right choice here since it is designed to be highly scalable, more than RDS or any other relational database service.

23. You accidently stopped an EC2 instance in a VPC with an associated Elastic IP. If you start the instance again, what will be the result?

Elastic IP will be only disassociated from the instance if it's terminated. If it's stopped and started, there won't be any change to instance and no data will be lost.

24. Your organization has around 50 IAM users. Now, it wants to introduce a new policy that will affect the access permissions of an IAM user. How can it implement this without having to apply the policy at the individual user level?

It is possible using AWS IAM groups, by adding users in the groups as per their roles and by simply applying the policy to the groups.

Advanced AWS Interview Questions

25. Your organization is using DynamoDB for its application. This application collects data from its users every 10 minutes and stores it in DynamoDB. Then every day, after a particular time interval, the data (respective to each user) is extracted from DynamoDB and sent to S3. Then, the application visualizes this data to the users. You are asked to propose a solution to help optimize the backend of the application for latency at lower cost. What would you recommend?

ElastiCache. Amazon ElastiCache is a caching solution offered by Amazon.

Elastic Cache

It can be used to store a cached version of the application in a region closer to users so that when requests are made by the users the cached version of the application can respond, and hence latency will be reduced.

26. I created a web application with autoscaling. I observed that the traffic on my application is the

highest on Wednesdays and Fridays between 9 AM and 7 PM. What would be the best solution for me to handle the scaling?

Configure a policy in autoscaling to scale as per the predictable traffic patterns.

27. How would you handle a situation where the relational database engine crashes often whenever the traffic to your RDS instances increases, given that the replica of RDS instance is not promoted as the master instance?

A bigger RDS instance type needs to be opted for handling large amounts of traffic, creating manual or automated snapshots to recover data in case the RDS instance goes down.

Learn more about Amazon Web Services from our AWS Tutorial!

28. You have an application running on your Amazon EC2 instance. You want to reduce the load on your instance as soon as the CPU utilization reaches 100 percent. How will you do that?

It can be done by creating an autoscaling group to deploy more instances when the CPU utilization exceeds 100 percent and distributing traffic among instances by creating a load balancer and registering the Amazon EC2 instances with it.

Watch this video on Free AWS Full Course:

29. What would I have to do if I want to access Amazon Simple Storage buckets and use the information for access audits?

AWS CloudTrail can be used in this case as it is designed for logging and tracking API calls, and it has also been made available for storage solutions.

Learn the complete concepts of AWS at Hyderabad in 26 hours!

30. I created a key in North Virginia region to encrypt my data in Oregon region. I also added three users to the key and an external AWS account. Then, to encrypt an object in S3, when I tried to use the same key, it was not listed. Where did I go wrong?

The data and the key should be in the same region. That is, the data that has to be encrypted should be in the same region as the one in which the key was created. In this case, the data is in Oregon region, whereas the key is created in North Virginia region.

31. Suppose, you hosted an application on AWS that lets the users render images and do some general computing. Which of the below listed services can you use to route the incoming user traffic?

Classic Load Balancer

Application Load Balancer

Network Load balancer

Application Load Balancer: It supports path-based routing of the traffic and hence helps in enhancing the performance of the application structured as smaller services.

Application Load Balancer

Using application load balancer, the traffic can be routed based on the requests made. In this case scenario, the traffic where requests are made for rendering images can be directed to the servers only deployed for rendering images and the traffic where the requests are made for computing can be directed to the servers deployed only for general computing purposes.

32. Suppose, I created a subnet and launched an EC2 instance in the subnet with default settings. Which of the following options will be ready to use on the EC2 instance as soon as it is launched?

Elastic IP

Private IP

Public IP

Internet Gateway

Private IP. Private IP is automatically assigned to the instance as soon as it is launched. While elastic IP has to be set manually, Public IP needs an Internet Gateway which again has to be created since it’s a new VPC.

33. Your organization has four instances for production and another four for testing. You are asked to set up a group of IAM users that can only access the four production instances and not the other four testing instances. How will you achieve this?

We can achieve this by defining tags on the test and production instances and then adding a condition to the IAM policy that allows access to specific tags.

34. Your organization wants to monitor the read and write IOPS for its AWS MySQL RDS instance and then send real-time alerts to its internal operations team. Which service offered by Amazon can help your organization achieve this scenario?

Amazon CloudWatch would help us achieve this. Since Amazon CloudWatch is a monitoring tool offered by Amazon, it's the right service to use in the above-mentioned scenario.

35. Which of the following services can be used if you want to capture client connection information from your load balancer at a particular time interval?

Enabling access logs on your load balancer

Enabling CloudTrail for your load balancer

Enabling CloudWatch metrics for your load balancer

Enabling CloudTrail for your load balancer. AWS CloudTrail is an inexpensive log monitoring solution provided by Amazon. It can provide logging information for load balancers or any other AWS resources. The provided information can further be used for analysis.

Learn more about AWS CloudWatch in the blog by Intellipaat.

36. You have created a VPC with private and public subnets. In what kind of subnet would you launch the database servers?

Database servers should be ideally launched in private subnets. Private subnets are ideal for the backend services and databases of all applications since they are not meant to be accessed by the users of the applications, and private subnets are not routable from the Internet.

37. Is it possible to switch from an Instance-backed root volume to an EBS-backed root volume at any time?

No, it is not possible.

38. Can you change the instance type of the instances that are running in your application tier and are also using autoscaling? If yes, then how? (Choose one of the following)

Yes, by modifying autoscaling launch configuration

Yes, by modifying autoscaling tags configuration

Yes, by modifying autoscaling policy configuration

No, it cannot be changed

Yes, the instance type of such instances can be changed by modifying the autoscaling launch configuration. The tags configuration is used to add metadata to the instances.

Do you know about the different types of AWS Certifications? Read the Blog to find out.

39. Can you name the additional network interface that can be created and attached to your Amazon EC2 instance launched in your VPC?

Elastic Network Interface

40. Out of the following options, where does the user specify the maximum number of instances with the autoscaling commands?

Autoscaling policy configuration

Autoscaling group

Autoscaling tags configuration

Autoscaling launch configuration

Autoscaling launch configuration

41. Which service provided by AWS can you use to transfer objects from your data center, when you are using Amazon CloudFront?

Amazon Direct Connect. It is an AWS networking service that acts as an alternative to using the Internet to connect customers in on-premise sites with AWS.

42. You have deployed multiple EC2 instances across multiple availability zones to run your website. You have also deployed a Multi-AZ RDS MySQL Extra Large DB Instance. The site performs a high number of small read and write operations per second. After some time, you observed that there is read contention on RDS MySQL. What would be your approach to resolve the contention and optimize your website?

We can deploy ElastiCache in-memory cache running in every availability zone. This will help in creating a cached version of the website for faster access in each availability zone. We can also add an RDS MySQL read replica in each availability zone that can help in efficient and better performance for read operations. So, there will not be any increased workload on the RDS MySQL instance, hence resolving the contention issue.

43. Your company wants you to propose a solution so that the company's data center can be connected to Amazon cloud network. What would be your proposal?

The data center can be connected to the Amazon cloud network by establishing a virtual private network (VPN) between the VPC and the data center. A virtual private network lets you establish a secure pathway or tunnel from your premise or device to AWS global network.

44. Which of the following Amazon Services would you choose if you want complex querying capabilities but not a whole data warehouse?

RDS

Redshift

ElastiCache

DynamoDB

Amazon RDS

45. You want to modify the security group rules while it is being used by multiple EC2 instances. Will you be able to do that? If yes, will the new rules be implemented on all previously running EC2 instances that were using that security group?

Yes, the security group that is being used by multiple EC2 instances can be modified. The changes will be implemented immediately and be applied to all the previously running EC2 instances without restarting the instances.

Become a Cloud and DevOps Architect

46. Which one of the following is a structured data store that supports indexing and data queries to both EC2 and S3?

DynamoDB

MySQL

Aurora

SimpleDB

SimpleDB

47. Which service offered by Amazon will you choose if you want to collect and process e-commerce data for near real-time analysis? (Choose any two)

DynamoDB

Redshift

Aurora

SimpleDB

DynamoDB. DynamoDB is a fully managed NoSQL database service that can be fed any type of unstructured data. Hence, DynamoDB is the aptest choice for collecting data from e-commerce websites. For near-real-time analysis, we can use Amazon Redshift.

48. If in CloudFront the content is not present at an edge location, what will happen when a request is made for that content?

CloudFront will deliver the content directly from the origin server. It will also store the content in the cache of the edge location where the content was missing.

49. Can you change the private IP address of an EC2 instance while it is in running or in a stopped state?

No, it cannot be changed. When an EC2 instance is launched, a private IP address is assigned to that instance at the boot time. This private IP address is attached to the instance for its entire lifetime and can never be changed.

50. Which of the following options will you use if you have to move data over long distances using the Internet, from instances that are spread across countries to your Amazon S3 bucket?

Amazon CloudFront

Amazon Transfer Acceleration

Amazon Snowball

Amazon Glacier

Amazon Transfer Acceleration. It throttles the data transfer up to 300 percent using optimized network paths and Amazon Content Delivery Network. Snowball cannot be used here as this service does not support cross-region data transfer.

51. Which of the following services is a data storage system that also has REST API interface and uses secure HMAC-SHA1 authentication keys?

Amazon Elastic Block Store

Amazon Snapshot

Amazon S3

Amazon S3. It gets various requests from applications, and it has to identify which requests are to be allowed and which are to be denied. Amazon S3 REST API uses a custom HTTP scheme based on a keyed HMAC for authentication of requests.

52. What is EC2?

Launched in 2006, EC2 is a virtual machine that you can use to deploy your own servers in the cloud, giving you OS-level control. It helps you have control over the hardware and updates, similar to the case of on-premise servers. EC2 can run on either of these operating systems- Microsoft and Linux. It can also support applications like Python, PHP, Apache, and more.

Learn more about AWS Secrets Manager in the blog by Intellipaat.

53. What is Snowball?

Snowball is an application designed for transferring terabytes of data into and outside of the AWS cloud. It uses secured physical storage to transfer the data. Snowball is considered as a petabyte-scale data transport solution that helps in cost and time-saving.

54. What is CloudWatch?

The Amazon CloudWatch is used for monitoring and managing data and getting actionable insights for AWS, on-premise applications, etc. It helps you to monitor your entire task stack that includes the applications, infrastructure, and services. Apart from this, CloudWatch also assists you in optimizing your resource utilization and cost by providing analytics-driven insights.

55. What is Elastic Transcoder?

In the AWS cloud, the Elastic Transcoder is used for converting media files into versions that can be run/played on devices such as Tablets, PCs, Smartphones, etc. It consists of advanced transcoding features with conversion rates starting from $ 0.0075 per minute.

Learn more about Amazon systems manager in the blog by intellipaat.

56. What do you understand by VPC?

VPC is the abbreviated form of Virtual Private Cloud. It allows you to launch AWS resources that can be defined by you and fully customize the network configurations. Through VPC, you can define and take full control of your virtual network environment. For example- you can have a private address range, internet gateways, subnets, etc.

57. What does an AMI include?

AMI stands for Amazon Machine Images. It includes the following:

Single or multiple Amazon Elastic Block Store (Amazon EBS) snapshots. Basically, templates for the root volume of the instance.

Launch permissions that let AWS accounts use AMI to launch instances.

A block device mapping to specify what volumes to be attached to the instance during its launch.

58. What are the Storage Classes available in Amazon S3?

The following storage classes are available in Amazon S3:

S3 Standard- It is by and large the default storage class. In cases where no specification about the storage class is provided while uploading the object, Amazon S3 assigns the S3 Standard storage class by default.

Reduced Redundancy- It is assigned when non-critical, reproducible data needs to be stored. The Reduced Redundancy Storage class is designed in a way that the above data categories can be stored with less redundancy.

However, it is always advisable to go ahead with the S3 Standard storage class.

59. What are the native AWS security logging capabilities?

The native AWS security logging capabilities include AWS CloudTrail, AWS Config, AWS detailed billing reports, Amazon S3 access logs, Elastic load balancing Access logs, Amazon CloudFront access logs, Amazon VPC Flow logs, etc. To know about native AWS security logging capabilities in detail, click here.

Take up the AWS Masters Certification Course by Intellipaat and upgrade your skillset.

60. What are key pairs?

When connecting to an Amazon EC2 instance, you need to prove your identity. Key pairs are used to execute this. Basically, a key pair is a set of security credentials that are used during identity proof. It

consists of a public key and a private key.

61. What are policies and what are the different types of policies?

Policies define the permissions required to execute an operation irrespective of the method used to perform it. AWS supports six types of policies:

Identity-based policies

Resource-based policies

Permissions boundaries

Organizations SCPs

ACLs

Session policies

1- Identity-based policies- They are JSON permissions policy documents that control what actions an identity can perform, under what conditions, and on which resources. These policies are further classified into 2 categories:

Managed Policies– These policies are standalone identity-based policies that can be attached to different users, groups in your AWS environment.

Inline policies- These policies are directly attached to a single user, group, or role. In situations where inline policies are used, a strict one-to-one relationship between a policy and an identity is maintained.

2- Resource-based policies- These policies are the ones attached to a resource such as an Amazon S3 bucket. They define which actions can be performed on the particular resource and under what circumstances.

3- IAM permissions boundaries- They actually refer to the maximum level of permissions that identity-based policies can grant to the specific entity.

4- Service Control Policies (SCPs)- SCPs are the maximum level of permissions for an organization or organizational unit.

5- Access Control lists- They define and control which principals in another AWS account can access the particular resource.

6- Session policies- They are advanced policies that are passed as a parameter when a temporary session is programmatically created for a role or federated user.

62. What kind of IP address can you use for your customer gateway (CGW) address?

We can use the Internet routable IP address, which is a public IP address of your NAT device.

If you have any doubts or queries related to AWS, get them clarified from AWS experts on our AWS Community!

63. Which of the following is not an option in security groups?

List of users

Ports

IP addresses

List of protocols

List of users

List of Users

Hope these top AWS Interview questions and answers for freshers and the experienced, helps you in preparing for top AWS jobs in the Cloud market.

AWS Scenario Based Questions

64. A Company has a running Web Application Server in the N. Virginia region and the server has a large size EBS volume of approximately 500 GB, and to see the demand of business, the company needs to migrate the server from the current region to another AWS account's Mumbai location. Which is the

best way to migrate the server from the current location to the Mumbai region? And what information AWS administrator does require about AWS A/C?

Create an AMI of the server running in the North Virginia region. Once the AMI is created, The administrator would need the 12 digit account number of the #2 AWS account. This is required for copying the AMI which we have created.

Once the AMI is successfully copied into the Mumbai region, you can launch the instance using copied AMI in the Mumbai region. Once the instance is running and if it's completely operational, the server in the North Virginia region could be terminated. This is the best way to migrate a server to a different account without any hassle.

65. Unable to ping Instance We launched a Windows 2019 IIS server in the Ohio region and deployed a dynamic website in this server, in addition, the webserver also connected with a backend MS-SQL server to store and access data related to the application. Our users were able to access the website over the Internet. The next day our client informed us that they were able to access the website, but weren't able to ping the server from the Internet. To ensure ICMP rule in Security Group, we checked, and the Security Group had allowed rule from 0.0.0.0/0. Would you try to help troubleshoot the issue?

If the client is able to access the website from his/her end, it means the connection is perfect and no issue with connectivity and the Security Group configuration also seems correct.

We can check the internal firewall of the Windows 2019 IIS server. If it is blocking ICMP traffic, we should enable it.

66. A start-up company has a web application based in the us-east-1 Region with multiple Amazon EC2 instances running behind an Application Load Balancer across multiple Availability Zones. As the company's user base grows in the us-west-1 region, the company needs a solution with low latency and improved high availability. What should a solutions architect do to achieve it.?

You need to notice here, currently, the web application is in us-ease-1, and the user base grows in the us-east-1 region. The very first step, provision multiple EC2 instances (web application servers) and configure an Application Load Balancer in us-west-1. Now, create Global Accelerator in AWS Global

Accelerator which uses an endpoint group that includes the load balancer endpoints in both Regions.

Read this blog about AWS services to know more.

67. A company currently operates 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?

Create a snapshot of the database.

Copy it to an encrypted snapshot.

Restore the database from the encrypted snapshot.

68. A company is going to launch one branch in the UK and need to continue with its existing main branch in the USA. The company has almost 15 GB of data which is stored in an S3 Bucket in the Ohio region and data is stored with the default storage class. The Company also wants to provide its updated & stored data in the London S3 bucket using one zone accessibility storage class to save storage costs. In addition, the company also wants that the data must be updated automatically in S3's London bucket; if any data is modified or written in the S3 bucket in Ohio.

Configure Cross Region Replication Rule in Ohio region bucket and select destination bucket in the London region to replicate the data and store it in destination using one zone IA storage class to save cost.

69. You are an AWS Architect in your company, and you are asked to create a new VPC in the N.Virginia Region with two Public and two Private subnets using the following CIDR blocks:

VPC CIDR = 10.10.10.0/24

Public Subnet

Subnet01 : 10.10.10.0/26

Subnet02 : 10.10.10.64/26

Private Subnet

Subnet03: 10.10.10.128/26

Subnet04: 10.10.10.192/26

Using the above CIDRs you created a new VPC, and you launched EC2 instances in all subnets as per the need.

Now, you are facing an issue in private instances that you are unable to update operating systems from the internet. So, what architectural changes and configurations will you suggest to resolve the issue?

NAT G/W to be installed in one public subnet and will configure the route-table associated with private subnets to add NAT G/W entry to provide internet access to private instances.

70. The data on the root volumes of store-backed and EBS-backed instances get deleted by default when they are terminated. If you want to prevent that from happening, which instance would you use? And ensure if the EC2 instance is restarted, the data or configuration in the EC2 instance should not be lost.

EBS-backed instances or instances with EBS Volume. EBS-backed instances use EBS volume as their root volume. These volumes contain Operating Systems, Applications, and Data. We can create Snapshots from these volumes or AMI from Snapshots.

The main advantage of EBS-backed volume is that the data can be configured to be stored for later retrieval even if the virtual machine or the instances are shut down.

71. You have an application running on an EC2 instance. You need to reduce the load on your instance as soon as the CPU utilization reaches 80 percent. How will you accomplish the job?

It can be done by creating an autoscaling group to deploy more instances when the CPU utilization of the EC2 instance exceeds 80 percent and distributing traffic among instances by creating an application load balancer and registering EC2 instances as target instances.

72. In AWS, three different storage services are available, such as EFS, S3, and EBS. When should I use Amazon EFS vs. Amazon S3 vs. Amazon Elastic Block Store (EBS)?

Amazon Web Services (AWS) offers cloud storage services to support a wide range of storage workloads.

Amazon EFS is a file storage service for use with Amazon compute (EC2, containers, serverless) and on-premises servers. Amazon EFS provides a file system interface, file system access semantics (such as strong consistency and file locking), and concurrently accessible storage for up to thousands of Amazon EC2 instances.

Amazon EBS is a block-level storage service for use with Amazon EC2. Amazon EBS can deliver performance for workloads that require the lowest latency access to data from a single EC2 instance.

Amazon S3 is an object storage service. Amazon S3 makes data available through an Internet API that can be accessed anywhere

73. A company's web application is using multiple Linux Amazon EC2 instances and storing data on Amazon EBS volumes. The company is looking for a solution to increase the resiliency of the application in case of a failure and to provide storage that complies with atomicity, consistency, isolation, and durability (ACID). What should a solutions architect do to meet these requirements?

Create an Application Load Balancer with AWS Auto Scaling groups across multiple Availability Zones. Store data on Amazon EFS and mount a target on each instance.

74. An application running on AWS uses an Amazon Aurora Multi-AZ deployment for its database. When evaluating performance metrics, a solutions architect discovered that the database reads are causing high I/O and adding latency to the write requests against the database. What should the solutions architect do to separate the read requests from the write requests?

Create a read replica and modify the application to use the appropriate endpoint.

75. A client reports that they wanted to see an audit log of any changes made to AWS resources in their account. What can the client do to achieve this?

Enable AWS CloudTrail logs to be delivered to an Amazon S3 bucket

76. Usually, you have noticed that one EBS volume can be connected with one EC2 instance, our company wants to run a business-critical application on multiple instances in a single region and need to store all instances output in single storage within the VPC. Instead of using EFS, our company is recommending the use of multi-attach volume with instances. As an architect, you need to suggest them what instance type and EBS volumes they should use.

The instance type should be EC2 Nitro-based instances and Provisioned IOPs io1 multi-attach EBS volumes.

77. A company is using a VPC peering connection option to connect its multiple VPCs in a single region to allow for cross VPC communication. A recent increase in account creations and VPCs has made it difficult to maintain the VPC peering strategy, and the company expects to grow to hundreds of VPCs. There are also new requests to create site-to-site VPNs with some of the VPCs. A solutions architect has been tasked with creating a centrally networking setup for multiple accounts and VPNs. Which networking solution would you recommend to resolve it?

Configure a transit gateway with AWS Transit Gateway and connect all VPCs and VPNs.

78. An organization has multiple facilities in various continents such as North America, Europe, and the Asia Pacific. The organization is designing a new distributed application to manage and optimize its global supply chain and its manufacturing process. It needs to design the process in such a way that the booked order in one continent should be able to support data failover with a short Recovery Time Objective (RTO). The uptime of the application should not impact manufacturing, what kind of solution would you recommend as a solution architect?

Use Amazon DynamoDB global tables feature for the database

Next