**AWS Interview Questions:**

1. **What do you know about AWS Region?**

* An AWS Region is a completely independent entity in a geographical area.
* There are two or more Availability Zones in an AWS Region.Within a region, Availability Zones are connected through low-latency links
* Since each AWS Region is isolated from another Region, it provides very high fault tolerance and stability. Within a region, resources of a service are independent.

1. **What are the important components of IAM?**

The important components of Identity and Access Management (IAM) are as follows:

* IAM User
* Group
* Role
* Policy

1. **What are the important points about AWS IAM**

Some of the important points about AWS IAM are as follows:

* A new User in IAM does not have any permission.
* AWS IAM assigns an Access Key and a Secret Access Key to a new User
* An Access Key cannot be used to login to AWS Console
* We use Access Key to access AWS via an API or Command Line interface (CLI).
* IAM is a universal application
* It is common across all the regions in AWS. When we first set up our AWS account, we get a root account that has complete Admin access.

1. **What are the important features of Amazon S3?**

Some of the important features of Amazon S3 are as follows:

* Amazon S3 provides unlimited storage for files.
* File size in Amazon S3 can vary from 0 Bytes to 5 Terabytes.
* The largest object (file) that can be uploaded to S3 in a single PUT request is upto 5 gigabytes.
* We have to store files in Buckets in Amazon S3. In Amazon S3, names of buckets have to be unique globally.
* Amazon S3 is an Object based storage. Internally, S3 uses a key based object store.
* When we store an object we assign a key that is used to uniquely identify the object.

1. **What is the scale of durability in Amazon S3?**

* Amazon S3 supports durability at the scale of 99.999999999% (11 9s)of time.
* This is 9 nines after decimal.
* It means there is a chance of losing 0.000000001% of objects being stored every year.

1. **What are the different tiers in Amazon S3 storage?**

Different Storage tiers in Amazon S3 are as follows:

* **S3 Standard:** In this tier, S3 supports durable storage of files that become immediately available.
* This tier is used for frequent file storage and access.
* **S3 Standard-Infrequent Access (IA):** In this tier, S3 provides durable storage that is immediately available.
* But in this tier files are infrequently accessed.
* **S3 Reduced Redundancy Storage (RRS):** In this tier, S3 provides the option to customers to store data at lower levels of redundancy.
* In this case, data is copied to multiple locations but not on as many locations as standard S3.
* **Glacier and DEEP\_ARCHIVE:** The new Glacier Deep Archive storage class is designed to provide durable and secure long-term storage for large amounts of data at a price that is competitive with off-premises tape archival services.
* Data is stored across 3 or more AWS Availability Zones and can be retrieved in 12 hours or less.

1. **What is an Object when we delete it from Amazon S3?**

* Amazon S3 provides DELETE API to delete an object.
* If we want to delete an object from a version controlled bucket, we can specify the version of the object that we want to delete.
* The other versions of the Object still exist within the bucket.
* If we do not specify the version, and just pass the key name, Amazon S3 will delete the object and return the version id. And the object will not appear on the bucket.
* In case Multi-factor authentication (MFA) is enabled on a bucket, the DELETE request will fail if we do not specify an MFA token.

1. **Explain the Amazon Glacier?**

* Amazon Glacier is an extremely low cost cloud based storage service provided by Amazon.
* We mainly use Amazon Glacier for long-term backup purpose.
* Amazon Glacier can be used for storing data archives for months, years or even decades.
* It can also be used for long term immutable storage for regulatory and archival requirements.
* It provides Vault Lock support for this purpose.
* In this option, we write once but can read the same data multiple times.
* One use case is for storing certificates that can be issued once, and only the original person can keep the main copy. But other users can view that copy of the certificate.

1. **Can we disable versioning on a version-enabled bucket in Amazon S3?**

* No, we cannot disable versioning on a version-enabled bucket in Amazon S3.
* We can just suspend the versioning on a bucket in S3.
* Once we suspend versioning, Amazon S3 will stop creating new versions of the object.
* It just stores the object with null version ID.
* When we overwrite an existing object, it just replaces the object with null version ID.
* Therefore, any existing versions of the object still remain in the bucket.
* But there will be no more new versions of the same object except the null version ID object.

1. **Can we do Cross Region replication in Amazon S3 without enabling versioning on a bucket?**

* No, we have to enable versioning on a bucket to perform Cross Region Replication.

1. **What is CloudFront?**

* Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users.
* CloudFront delivers your content through a worldwide network of data centers called edge locations.

1. **What are the main features of Amazon CloudFront?**

Some of the main features of Amazon CloudFront are as follows:

* Device Detection
* Protocol Detection
* Geo Targeting
* Cache Behavior
* Cross Origin Resource Sharing
* Multiple Origin Servers
* HTTP Cookies
* Query String Parameters
* Custom SSL

1. **Is it Amazon S3 is Secure if yes then how?**

Amazon S3 is a very secure storage service. Some of the main security mechanisms available in Amazon S3 are as follows:

* **Access:** When we create a bucket or an object, only the owner gets the access to the bucket and objects.
* **Authentication:** Amazon S3 also supports user authentication to control who has access to a specific object or bucket.
* **Access Control List:** We can create Access Control Lists (ACL) to provide selective permissions to users and groups for S3 objects.
* **HTTPS:** Amazon S3 also supports HTTPS protocol to securely upload and download data from the cloud.
* **Encryption:** We can also use Server Side Encryption (SSE) in Amazon S3 to encrypt data.

1. **What is the difference between spot instances and On-demand instances?**

Spot Instance and On-demand Instance are very similar in nature. The main difference between these is commitment.

* **In Spot Instance**, there is no commitment. As soon as the Bid price exceeds Spot price, a user gets the Instance.
* In an **On-demand Instance**, a user has to pay the On-demand rate specified by Amazon. Once they have bought the Instance they have to use it by paying that rate.
* In **Spot Instance**, once the Spot price exceeds the Bid price, Amazon will shut the instance. The benefit to users is that they will not be charged for the partial hour in which Instance was taken back from them.

1. **What are the different types of load balancing options provided by aws?**

Amazon Elastic Load Balancing (ELB) provides the following types of load balancers:

* **Classic Load Balancer:** This Load Balancer uses application or network load information to route traffic. It is a simple approach of load balancing to divide load among multiple EC2 instances.
* **Application Load Balancer:** This Load Balancer uses advanced application level information to route the traffic among multiple EC2 instances.
* It can even use the content of the request to make routing decisions.
* **Network Load Balancer:** The network load balancer is used for balancing the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) traffic. It can handle millions of requests per second.

1. **Which Load balancer do you use in your project?**
2. **What kind of volume is provided by Amazon?**

* Amazon EBS provides following two main types of Volume:
* **Solid State Drive (SSD):** This type of Volume is backed by a Solid State Drive.
* It is suitable for transactional work in which there are frequent reads and writes.
* It is generally more expensive than the HDD based volume.
* **Hard Disk Drive (HDD):** This type of Volume is backed by Hard Disk Drive.
* It is more suitable for large streaming workloads in which throughput is more important than transactional work.
* It is a cheaper option compared to SSD Volume.

1. **Tell me the difference between Instance store and EBS**

* Some of the Amazon EC instance types provide the option of using a directly attached block-device storage. This kind of storage is known as an Instance Store. In other Amazon EC2 instances, we have to attach an Elastic Block Store (EBS).
* **Persistence:** The main difference between Instance Store and EBS is that in Instance Store data is not persisted for long-term use.
* If the Instance terminates or fails, we can lose Instance Store data.
* Any data stored in EBS is persisted for a longer duration. Even if an instance fails, we can use the data stored in EBS to connect it to another EC2 instance.
* **Encryption:** EBS provides a full-volume encryption of data stored in it. Whereas, Instance Store is not considered as a good storage option for encrypted data.

1. **What is Elastic IP?**

* Amazon provides an Elastic IP Address with an AWS account.
* An Elastic IP address is a public and static IP address based on IPv4 protocol.
* It is designed for dynamic cloud computing.
* This IP address is reachable from the Internet. If we do not have a specific IP address for our EC2 instance, then we can associate our instance to the Elastic IP address of our AWS account.
* Now our instance can communicate on the Internet with this Elastic IP Address.

1. **What are the different routing policies available in Route 53?**

Route 53 service from Amazon provides multiple options for creating a Routing policy. Some of these options are as follows:

* **Simple Routing:** In this option, Route 53 will respond to DNS queries based on the values in the resource record set.
* **Weighted Routing:** In this policy, we can specify the weightage according to which multiple resources will handle the load. E.g. If we have two web servers, we can divide the load in a 40/60 ratio on these servers.
* **Latency Routing:** In this option, Route 53 will respond to DNS queries with the resources that provide the best latency.
* **Failover Routing:** We can configure active/passive failover by using this policy. One resource will get all the traffic when it is up. Once the first resource is down, all the traffic will be routed to the second resource that is active during failover.
* **Geolocation Routing:** As the name suggests, this policy works on the basis of location of end users from where requests originate.

1. **How does Amazon Route 53 provide high available and low latency?**

* Route 53 is built using AWS’s highly available and reliable infrastructure.
* The globally distributed nature of our DNS servers helps ensure a consistent ability to route your end users to your application by circumventing any internet or network related issues.
* Route 53 is designed to provide the level of dependability required by important applications.
* Using a global anycast network of DNS servers around the world, Route 53 is designed to automatically answer queries from the optimal location depending on network conditions. As a result, the service offers low query latency for your end users.

1. **What does AMI include?**

**An AMI includes the following:**

* One or more Amazon Elastic Block Store (Amazon EBS) snapshots, or, for instance-store-backed AMIs, a template for the root volume of the instance (for example, an operating system, an application server, and applications).
* Launch permissions that control which AWS accounts can use the AMI to launch instances.
* A block device mapping that specifies the volumes to attach to the instance when it's launched.

1. **What are the different types of Instances?**

Here are different types of EC2 instance:

* General Purpose Instances
* Compute Optimized Instances
* Memory Optimized Instances
* Accelerated Computing Instances
* Storage Optimized Instances

1. **What are the different types of EC2 instances based on their cost**

Amazon EC2 is free to try. There are five ways to pay for Amazon EC2 instances:

* [On-Demand](https://aws.amazon.com/ec2/pricing/on-demand/)
* [Savings Plans](https://aws.amazon.com/savingsplans/)
* [Reserved Instances](https://aws.amazon.com/ec2/pricing/reserved-instances/)
* [Spot Instances](https://aws.amazon.com/ec2/spotathon/)
* You can also pay for [Dedicated Hosts](https://aws.amazon.com/ec2/dedicated-hosts/) which provide you with EC2 instance capacity on physical servers dedicated for your use.

1. **What is a Stateful and Stateless Firewall?**

**Security groups are stateful:**

* This means any changes applied to an incoming rule will be automatically applied to the outgoing rule.
* e.g. If you allow an incoming port 80, the outgoing port 80 will be automatically opened.

**Network ACLs are stateless:**

* This means any changes applied to an incoming rule will not be applied to the outgoing rule.
* e.g. If you allow an incoming port 80, you would also need to apply the rule for outgoing traffic.

1. **Is there a way to upload a file that is greater than 100 Megabytes in Amazon S3?**

* Amazon S3 supports storing of objects or files up to 5 gigabytes in a single PUT request.
* To upload a file greater than 100 megabytes, we have to use Multipart upload utility from AWS. By using Multipart upload we can upload a large file in multiple parts.
* Each part will be independently uploaded to S3. It doesn’t matter in what order each part is uploaded.
* It even supports uploading these parts in parallel to decrease overall time. Once all the parts are uploaded, this utility joins these parts as a single object or file from which the parts were created.
* **Refer Link:** https://aws.amazon.com/premiumsupport/knowledge-center/s3-upload-large-files/

1. **Can you change the private IP Address of an EC2 instance while it is running or in a Stopped state?**

* The private IP address of an Amazon EC2 instance will never change.
* It will not change while an instance is running.
* It will not change while an instance is stopped.
* You cannot change a private IP address. (However, I think that if you assign multiple private IP addresses, you can add/remove the secondary addresses, but not the primary IP address.)
* You cannot launch another instance with the same private IP address of another instance (in the same VPC), even if the other instance is stopped.
* The above only applies to the private IP address, not the public IP address.

1. **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.

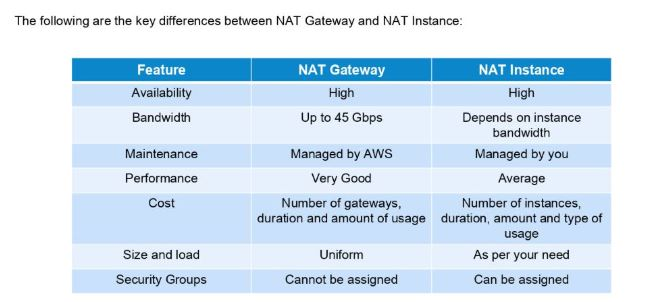
1. **How do you set up a System to monitor website metrics in real time in AWS?**
2. **Name some of the AWS Services that are not region specific.**

AWS services that are not region-specific are:

* IAM
* Route 53
* Web Application Firewall
* CloudFront

1. **What are the difference between NAT Gateways and NAT Instances?**

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



1. **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.

1. **Can S3 be used with EC2 instances and if yes then 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.

1. **How do you Configure Cloud Watch to recover EC2 instances?**

* Open the [Amazon EC2 console](https://console.aws.amazon.com/ec2/).
* In the navigation pane, choose Instances.
* Select the instance that you want to configure.
* Choose Actions, and then choose Monitor and troubleshoot. Then, choose Manage CloudWatch alarms.
* Choose Create an alarm.  
  Note: To create an alarm, you must have AWS Identity and Access Management (IAM) permissions to stop and start the associated instance. For more information, see [Creating IAM roles](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create.html).
* For Alarm notification, choose an existing Amazon Simple Notification Service (Amazon SNS) topic. To create a new topic, see [Creating an Amazon SNS topic](https://docs.aws.amazon.com/sns/latest/dg/sns-create-topic.html).  
  Note: To receive notifications when an alarm is triggered, you must be [subscribed to the SNS topic](https://docs.aws.amazon.com/sns/latest/dg/sns-create-subscribe-endpoint-to-topic.html).
* Toggle on Alarm action, and then choose Recover.
* For Group samples by and Type of data to sample, choose an appropriate statistic and metric for your use case.
* For Consecutive period and Period, specify the evaluation period for the alarm.
* (Optional) Modify the automatically created Alarm name.
* Choose Create.

1. **What are common types of AMI designs?**

All organizations should have a documented process for provisioning server images to ensure images can be recreated and easily updated in adherence to corporate standards. When determining what to include in an AMI, consider the following AMI design best practices:

* Avoid embedding passwords, private keys, or other sensitive information in AMIs.
* Leverage AWS CloudFormation or a third-party configuration management tool to document and automate AMI creation and updating.
* Create a library of reusable, modular templates that can be programmatically assembled to create different types of AMIs.
* Instrument AMIs with a standard bootstrapping capability that allows the instance to reference runtime information at launch.
* Develop a consistent strategy for tagging AMIs to allow for the easy organization and identification of images and their contents.

1. **What are the key-pairs in aws? If you lose the key what will happen or how to get the ec2-instance?**

**Refer Link:** https://aws.amazon.com/premiumsupport/knowledge-center/user-data-replace-key-pair-ec2/

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

## **Resolution**

Follow these steps to update a user's IAM permissions for console access to only a certain bucket or folder:

1. Open the [IAM console](https://console.aws.amazon.com/iam/).

2. From the console, open the IAM user or role that should have access to only a certain bucket.

3. In the Permissions tab of the IAM user or role, expand each policy to view its JSON policy document.

4. In the JSON policy documents, search for the policy that grants the user permission to the s3:ListAllMyBuckets action or to s3:\* actions (all S3 actions).

5. [Modify the policy](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_change-permissions.html) to remove permission to the s3:ListAllMyBuckets action.

Note: If an attached user policy is allowing s3:\* or Full Admin access with the "\*" resource, then the policy already includes the s3:ListAllMyBuckets permissions. Therefore, remove the "\*" resource. Instead, make sure that you're using one of the example policies listed in this article.

6. Add permission to s3:ListBucket only for the bucket or folder that you want the user to access from the console.

The following example policy is for access to an S3 bucket:

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": [

"s3:ListBucket"

],

"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"

},

{

"Effect": "Allow",

"Action": [

"s3:PutObject",

"s3:GetObject"

],

"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/\*"

}

]

}

The policy allows the user to perform the s3:ListBucket, s3:PutObject, and s3:GetObject actions only on DOC-EXAMPLE-BUCKET.

The following example policy grants access to a folder. The policy allows the user to perform the s3:ListBucket, s3:ListBucketVersions, s3:PutObject, s3:GetObject, and s3:GetObjectVersion actions only on folder2 within DOC-EXAMPLE-BUCKET. s3:ListBucketVersions and s3:GetObjectVersion are required only if the bucket has versioning turned on and you want users to have access to prior versions of objects.

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "AllowUsersToAccessFolder2Only",

"Effect": "Allow",

"Action": [

"s3:GetObject",

"s3:GetObjectVersion",

"s3:PutObject"

],

"Resource": [

"arn:aws:s3:::DOC-EXAMPLE-BUCKET/folder1/folder2/\*"

]

},

{

"Effect": "Allow",

"Action": [

"s3:ListBucket",

"s3:ListBucketVersion"

],

"Resource": [

"arn:aws:s3:::DOC-EXAMPLE-BUCKET"

],

"Condition": {

"StringLike": {

"s3:prefix": [

"folder1/folder2/\*"

]

}

}

}

]

}

7. Provide the user with a direct console link to the S3 bucket or folder. The direct console link to an S3 bucket looks like this:

https://s3.console.aws.amazon.com/s3/buckets/DOC-EXAMPLE-BUCKET/

The direct console link to a folder looks like this:

https://s3.console.aws.amazon.com/s3/buckets/DOC-EXAMPLE-BUCKET/folder1/folder2/

The user must use the direct link to be able to access the S3 bucket or folder from the console.

1. **What are the elements of AWS VPC?**

In AWS the VPC consists of the following components:

* **Subnet:** A segment of a VPC’s where you can place groups to isolated resources.
* **Internet Gateway:** VPC side of a connection to utilize public Internet.
* **NAT Gateway:** A highly available, managed Network Address Translation (NAT) service for your resources in a private subnet to access the Internet.
* **Virtual private gateway:** The Amazon VPC side of a VPN connection for secure transactions.
* **Peering Connection:** To route traffic via private IP addresses between two peered VPCs.
* **VPC Endpoints:** Enables private connectivity for your service in AWS without using an Internet Gateway, VPN, Network Address Translation (NAT) devices, or firewall proxies.
* **Egress-only Internet Gateway:** A stateful gateway that provides egress only access for IPv6 traffic from the VPC to the Internet.

1. **How to build a custom VPC?**
2. **What do you know about VPC Peering?**
3. **What are the differences between Private, public and Elastic IP addresses ?**
4. **Is there any limit to the number of VPC, subnets, gateways, VPNs that I can create?**

**Number of VPC:**

* VPCs per Region default is 5
* You can increase this limit so that you can have 100s of VPCs per Region.

**Subnets:**

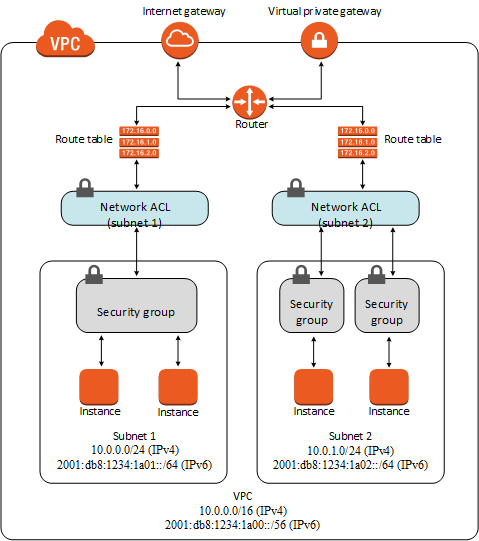
* Subnets per VPC default 200

**Gateways:**

* Egress only internet gateways per Region default is 5
* Internet Gateways per Region default is 5
* NAT Gateways per Availability zone default is 5

**Refer Link: https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html**

1. **Difference between Security Group and NACL?**

****

**Refer link: https://docs.aws.amazon.com/vpc/latest/userguide/VPC\_Security.html**

1. **What is Horizontal scaling?**

Autoscaling is the process of automatically increasing or decreasing the computational resources delivered to a cloud workload based on need

AWS auto scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost.

Before answer the Horizontal Scaling discuss below points

* Scale Out: Increase the instance, when traffic increases.
* Scale in: Terminates the instances when traffic is down.
* Above process is called horizontal scaling i.e. scale out and scale in.

1. **Can you explain how auto scaling works?**
2. **Difference between NLB vs ALB**
3. **Does Route53 do load balancing**
4. **Region based user**