

AWS

419. What do you know about AWS Region?

An AWS Region is a completely independent entity in a geographical area. There are two 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.

For launching an EC2 instance, we have to select an AMI within the same region.

420. What are the important components of IAM?

The important components of IAM are as follows:

- 1.
- 2.
- 3.
- 4.

IAM User: An IAM User is a person or service that will interact with AWS. User can sign into AWS Management Console for performing tasks in AWS.

IAM Group: An IAM Group is a collection of IAM users. We can specify permission to an IAM Group. This helps in managing large number of IAM users. We can simply add or remove an IAM User to an IAM Group to manage the permissions.

IAM Role: An IAM Role is an identity to which we give permissions. A Role does not have any credentials (password or access keys). We can temporarily give an IAM Role to an IAM User to perform certain tasks in AWS.

IAM Permission: In IAM we can create two types of Permissions. Identity based and Resource based. We can create a Permission to access or perform an action on an AWS Resource and assign it to a User, Role or Group. We can also create Permissions on resources like S3 bucket, Glacier vault etc and specify who has access to the resource.

IAM Policy: An IAM Policy is a document in which we list permissions to specify Actions, Resources and Effects. This document is in JSON format. We can attach a Policy to an IAM User or Group.

- 5.

421. What are the important points about AWS IAM?

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

1. A new User in IAM does not have any permission.
2. AWS IAM assigns an Access Key and a Secret Access Key to a new User.
3. An Access Key cannot be used to login to AWS Console.
4. We use Access Key to access AWS via an APIs or Command Line interface.
5. IAM is a universal application. It is common across all the regions in AWS.
6. When we first setup our AWS account, we get a root account that has complete Admin access.

422. What are the important features of Amazon S3?

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

1. Amazon S3 provides unlimited storage for files.
2. File size in Amazon S3 can vary from 0 Bytes to 5 Terabytes.
3. We have store files in Buckets in Amazon S3.
4. In Amazon S3, names of buckets have to be unique globally.

5. Amazon S3 is Object Based storage.

423. What is the scale of durability in Amazon S3?

Amazon S3 supports durability at the scale of 99.999999999% of time. This is 9 nines after decimal.

424. What are the Consistency levels supported by Amazon S3?

Amazon S3 supports Read after Write consistency when we create a new object by PUT. It means as soon as we Write a new object, we can access it.

Amazon S3 supports Eventual Consistency when we overwrite an existing object by PUT. Eventual Consistency means that the effect of overwrite will not be immediate but will happen after some time.

For deletion of an object, Amazon S3 supports Eventual Consistency after DELETE.

425. What are the different tiers in Amazon S3 storage?

Different Storage tiers in Amazon S3 are as follows:

1. **S3 Standard:** In this tier, S3 supports durable storage of files that become immediately available. This is used for frequently used files.
2. **S3 Standard -Infrequent Access (IA):** In this tier, S3 provides durable storage that is immediately available. But in this tier files are infrequently accessed.
3. **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.

426. How will you upload a file greater than 100 megabytes in Amazon S3?

Amazon S3 supports storing objects or files up to 5 terabytes. 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. 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 makes these as one single object or file from which the parts were created.

427. What happens to an Object when we delete it from Amazon S3?

Amazon S3 provides DELETE API to delete an object.

If the bucket in which the object exists is version controlled, then 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 the bucket is Multi-factor authentication (MFA) enabled, then the DELETE request will fail if we do not specify a MFA token.

428. What is the use of 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 based on regulatory and archiving requirements. It provides Vault Lock support for this purpose. In this option, we write once but can read many times same data.

One use case is for storing certificates that can be issued only once and only the original person keeps the main copy.

429. 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.

On overwriting an existing object, it just replaces the object with null version ID. So any existing versions of the object still remain in the bucket. But there will be no more new versions of the same object except for the null version ID object.

430. What are the use cases of Cross Region Replication Amazon S3?

We can use Cross Region Replication Amazon S3 to make copies of an object across buckets in different AWS Regions. This copying takes place automatically and in an asynchronous mode.

We have to add replication configuration on our source bucket in S3 to make use of Cross Region Replication. It will create exact replicas of the objects from source bucket to destination buckets in different regions.

Some of the main use cases of Cross Region Replication are as follows:

1. **Compliance:** Some times there are laws/regulatory requirements that ask for storing data at farther geographic locations. This kind of compliance can be achieved by using AWS Regions that are spread across the world.
2. **Failover:** At times, we want to minimize the probability of system failure due to complete blackout in a region. We can use Cross- Region Replication in such a scenario.
3. **Latency:** In case we are serving multiple geographies, it makes sense to replicate objects in the geographical Regions that are closer to end customer. This helps in reducing the latency.

431. 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.

432. What are the different types of actions in Object Lifecycle Management in Amazon S3?

There are mainly two types of Object Lifecycle Management actions in Amazon S3.

1. **Transition Actions:** These actions define the state when an Object transitions from one storage class to another storage class. E.g. a new object may transition to STANDARD_IA (infrequent access) class after 60 days of creation. And it can transition to GLACIER after 180 days of creation.
2. **Expiration Actions:** These actions specify what happens when an Object expires. We can ask S3 to delete an object completely on expiration.

433. How do we get higher performance in our application by using Amazon CloudFront?

If our application is content rich and used across multiple locations, we can use Amazon CloudFront to increase its performance. Some of the techniques used by Amazon CloudFront are as follows:

Caching: Amazon CloudFront caches the copies of our application's content at locations closer to our viewers. By this caching our users get our content very fast. Also due to caching the load on our main server decreases.

Edge / Regional Locations: CloudFront uses a global network of Edge and Regional edge locations to cache our content. These locations cater to almost all of the geographical areas across the world.

Persistent Connections: In certain cases, CloudFront keeps persistent connections with the main server to fetch the content quickly.

Other Optimization: Amazon CloudFront also uses other optimization techniques like TCP initial congestion window etc to deliver high performance experience.

434. What is the mechanism behind

Regional Edge Cache in Amazon

CloudFront?

A Regional Edge Cache location lies between the main webserver and the global edge location. When the popularity of an object/content decreases, the global edge location may take it out from the cache.

But Regional Edge location maintains a larger cache. Due to this the object/content can stay for long time in Regional Edge location. Due to this CloudFront does not have to go back to main webserver. When it does not find any object in Global Edge location it just looks for in Regional Edge location.

This improves the performance for serving content to our users in Amazon CloudFront.

435. What are the benefits of Streaming content?

We can get following benefits by Streaming content:

1. **Control:** We can provide more control to our users for what they want to watch. In a video streaming, users can select the locations in video where they want to start watching from.
2. **Content:** With streaming our entire content does not stay at a user's device. Users gets only the part they are watching. Once the session is over, content is removed from the user's device.
3. **Cost:** With streaming there is no need to download all the content to a user's device. A user can start viewing content as soon as some part is available for viewing. This saves costs since we do not have to download a large media file before starting each viewing session.

436. What is Lambda@Edge in AWS?

In AWS, we can use Lambda@Edge utility to solve the problem of low network latency for end users.

In Lambda@Edge there is no need to provision or manage servers. We can just upload our Node.js code to AWS Lambda and create functions that will be triggered on CloudFront requests.

When a request for content is received by CloudFront edge location, the Lambda code is ready to execute.

This is a very good option for scaling up the operations in CloudFront without managing servers.

437. What are the different types of

events triggered by Amazon

CloudFront?

Different types of events triggered by Amazon CloudFront are as follows:

1. **Viewer Request:** When an end user or a client program makes an HTTP/HTTPS request to CloudFront, this event is triggered at the Edge Location closer to the end user.
2. **Viewer Response:** When a CloudFront server is ready to respond to a request, this event is triggered.
3. **Origin Request:** When CloudFront server does not have the requested object in its cache, the request is forwarded to Origin server. At this time this event is triggered.
4. **Origin Response:** When CloudFront server at an Edge location receives the response from Origin server, this event is triggered.

438. What is Geo Targeting in Amazon CloudFront?

In Amazon CloudFront we can detect the country from where end users are requesting our content. This information can be passed to our Origin server by Amazon CloudFront. It is sent in a new HTTP header.

Based on different countries we can generate different content for different versions of the same content. These versions can be cached at different Edge Locations that are closer to the end users of that country.

In this way we are able to target our end users based on their geographic locations.

439. What are the main features of Amazon CloudFront?

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

1. 2. 3. 4. 5. 6. 7.

8. 9.

Device Detection

Protocol Detection

Geo Targeting

Cache Behavior

Cross Origin Resource Sharing Multiple Origin Servers

HTTP Cookies

Query String Parameters

Custom SSL

440. What are the security mechanisms available in Amazon S3?

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

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

Cloud Computing

441. What are the benefits of Cloud Computing?

There are ten main benefits of Cloud Computing:

Flexibility: The businesses that have fluctuating bandwidth demands need the flexibility of Cloud Computing. If you need high bandwidth, you can scale up your cloud capacity. When you do not need high bandwidth, you can just scale down. There is no need to be tied into an inflexible fixed capacity infrastructure.

Disaster Recovery: Cloud Computing provides robust backup and recovery solutions that are hosted in cloud. Due to this there is no need to spend extra resources on homegrown disaster recovery. It also saves time in setting up disaster recovery.

Automatic Software Updates: Most of the Cloud providers give automatic software updates. This reduces the extra task of installing new software version and always catching up with the latest software installs.

Low Capital Expenditure: In Cloud computing the model is Pay as you Go. This means there is very less upfront capital expenditure. There is a variable payment that is based on the usage.

Collaboration: In a cloud environment, applications can be shared between teams. This increases collaboration and communication among team members.

Remote Work: Cloud solutions provide flexibility of working remotely. There is no on site work. One can just connect from anywhere and start working.

Security: Cloud computing solutions are more secure than regular onsite work. Data stored in local servers and computers is prone to security attacks. In Cloud Computing, there are very few loose ends. Cloud providers give a secure working environment to its users.

Document Control: Once the documents are stored in a common repository, it increases the visibility and transparency among companies and their clients. Since there is one shared copy, there are fewer chances of discrepancies.

Competitive Pricing: In Cloud computing there are multiple players, so they keep competing among themselves and provide very good pricing. This comes out much cheaper compared to other options.

Environment Friendly: Cloud computing saves precious environmental resources also. By not blocking the resources and bandwidth.

442. What is On-demand computing in Cloud Computing?

On-demand Computing is the latest model in enterprise systems. It is related to Cloud computing. It means IT resources can be provided on demand by a Cloud provider.

In an enterprise system demand for computing resources varies from time to time. In such a scenario, On-demand computing makes sure that servers and IT resources are provisioned to handle the increase/decrease in demand.

A cloud provider maintains a pool of resources. The pool of resources contains networks, servers, storage, applications and services. This pool can serve the varying demand of resources and computing by various enterprise clients.

There are many concepts like- grid computing, utility computing, autonomic computing etc. that are similar to on-demand computing.

This is the most popular trend in computing model as of now.

443. What are the different layers of Cloud computing?

Three main layers of Cloud computing are as follows:

Infrastructure as a Service (IAAS): IAAS providers give low-level abstractions of physical devices. Amazon Web Services (AWS) is an example of IAAS. AWS provides EC2 for computing, S3 buckets for storage etc. Mainly the resources in this layer are hardware like memory, processor speed, network bandwidth etc.

Platform as a Service (PAAS): PAAS providers offer managed services like Rails, Django etc. One good example of PAAS is Google App Engineer. These are the environments in which developers can develop sophisticated software with ease.

Developers just focus on developing software, whereas scaling and performance is handled by PAAS provider.

Software as a Service (SAAS): SAAS provider offer an actual working software application to clients. Salesforce and Github are two good examples of SAAS. They hide the underlying details of the software and just provide an interface to work on the system. Behind the scenes the version of Software can be easily changed.

444. What resources are provided by Infrastructure as a Service (IAAS) provider?

An IAAS provider can give physical, virtual or both kinds of resources. These resources are used to build cloud.

IAAS provider handles the complexity of maintaining and deploying these services.

IAAS provider also handles security and backup recovery for these services. The main resources in IAAS are servers, storage, routers, switches and other related hardware etc.

445. What is the benefit of Platform as a Service?

Platform as a service (PaaS) is a kind of cloud computing service. A PaaS provider offers a platform on which clients can develop, run and manage applications without the need of building the infrastructure.

In PAAS clients save time by not creating and managing infrastructure environment associated with the app that they want to develop.

446. What are the main advantages of PaaS?

The advantages of PaaS are:

It allows development work on higher level programming with very less complexity.

Teams can focus on just the development of the application that makes the application very effective.

Maintenance and enhancement of the application is much easier.

It is suitable for situations in which multiple developers work on a single project but are not co-located.

447. What is the main disadvantage of PaaS?

Biggest disadvantage of PaaS is that a developer can only use the tools that PaaS provider makes available. A developer cannot use the full range of conventional tools.

Some PaaS providers lock in the clients in their platform. This also decreases the flexibility of clients using PaaS.

448. What are the different deployment models in Cloud computing?

Cloud computing supports following deployment models:

Private Cloud: Some companies build their private cloud. A private cloud is a fully functional platform that is owned, operated and used by only one organization.

Primary reason for private cloud is security. Many companies feel secure in private cloud. The other reasons for building private cloud are strategic decisions or control of operations.

There is also a concept of Virtual Private Cloud (VPC). In VPC, private cloud is built and operated by a hosting company. But it is exclusively used by one organization.

Public Cloud: There are cloud platforms by some companies that are open for general public as well as big companies for use and deployment. E.g. Google Apps, Amazon Web Services etc.

The public cloud providers focus on layers and application like- cloud application, infrastructure management etc. In this model resources are shared among different organizations.

Hybrid Cloud: The combination of public and private cloud is known as Hybrid cloud. This approach provides benefits of both the approaches- private and public cloud. So it is very robust platform.

A client gets functionalities and features of both the cloud platforms. By using Hybrid cloud an organization can create its own cloud as well as they can pass the control of their cloud to another third party.

449. What is the difference between Scalability and Elasticity?

Scalability is the ability of a system to handle the increased load on its current hardware and software resources. In a highly scalable system it is possible to increase the workload without increasing the re-

source capacity. Scalability supports any sudden surge in the demand/traffic with current set of resources.

Elasticity is the ability of a system to increase the workload by increasing the hardware/software resources dynamically. Highly elastic systems can handle the increased demand and traffic by dynamically commission and decommission resources. Elasticity is an important characteristic of Cloud Computing applications. Elasticity means how well your architecture is adaptable to workload in real time.

E.g. If in a system, one server can handle 100 users, 2 servers can handle 200 users and 10 servers can handle 1000 users. But in case for adding every X users, if you need 2X the amount of servers, then it is not a scalable design.

Let say, you have just one user login every hour on your site. Your one server can handle this load. But, if suddenly, 1000 users login at once, can your system quickly start new web servers on the fly to handle this load? Your design is elastic if it can handle such sudden increase in traffic so quickly.

450. What is Software as a Service?

Software as Service is a category of cloud computing in which Software is centrally hosted and it is licensed on a subscription basis. It is also known as On-demand software. Generally, clients access the software by using a thin- client like a web browser.

Many applications like Google docs, Microsoft office etc. provide SaaS model for their software.

The benefit of SaaS is that a client can add more users on the fly based on its current needs. And client does not need to install or maintain any software on its premises to use this software.

451. What are the different types of Datacenters in Cloud computing?

Cloud computing consists of different types of Datacenters linked in a grid structure. The main types of Datacenters in Cloud computing are:

Containerized Datacenter

As the name suggests, containerized datacenter provides high level of customization for an organization. These are traditional kind of datacenters. We can choose the different types of servers, memory, network and other infrastructure resources in this datacenter. Also we have to plan temperature control, network management and power management in this kind of datacenter.

Low-Density Datacenters

In a Low-density datacenter, we get high level of performance. In such a datacenter if we increase the density of servers, the issue with power comes. With high density of servers, the area gets heated. In such a scenario, effective heat and power management is done. To reach high level of performance, we have to optimize the number of servers' in the datacenter.

452. Explain the various modes of Software as a Service (SaaS) cloud environment?

Software as a Service (SaaS) is used to offer different kinds of software applications in a Cloud environment. Generally these are offered on subscription basis. Different modes of SaaS are:

Simple multi-tenancy: In this setup, each client gets its own resources. These resources are not shared with other clients. It is more secure option, since there is no sharing of resources. But it is an inefficient option, since for each client more money is needed to scale it with the rising demands. Also it takes time to scale up the application in this mode.

Fine grain multi-tenancy: In this mode, the feature provided to each client is same. The resources are shared among multiple clients. It is an efficient mode of cloud service, in which data is kept private among different clients but computing resources are shared. Also it is easier and quicker to scale up the SaaS implementation for different clients.

453. What are the important things to care about in Security in a cloud environment?

In a cloud-computing environment, security is one of the most important aspects.

With growing concern of hacking, every organization wants to make its software system and data secure. Since in a cloud computing environment, Software and hardware is not on the premises of an organization, it becomes more important to implement the best security practices.

Organizations have to keep their Data most secure during the transfer between two locations. Also they have to keep data secure when it is stored at a location. Hackers can hack into application or they can get an unauthorized copy of the data. So it becomes important to encrypt the data during transit as well as during rest to protect it from unwanted hackers.

454. Why do we use API in cloud computing environment?

Application Programming Interfaces (API) is used in cloud computing environment for accessing many services. APIs are very easy to use. They provide a quick option to create different set of applications in cloud environment.

An API provides a simple interface that can be used in multiple scenarios.

There are different types of clients for cloud computing APIs. It is easier to serve different needs of multiple clients with APIs in cloud computing environment.

455. What are the different areas of Security Management in cloud?

Different areas of Security management in cloud are as follows:

Identity Management: This aspect creates different level of users, roles and their credentials to access the services in cloud.

Access Control: In this area, we create multiple levels of permissions and access areas that can be given to a user or role for accessing a service in cloud environment.

Authentication: In this area, we check the credentials of a user and confirm that it is the correct user. Generally this is done by user password and multi-factor authentication like-verification by a one-time use code on cell phone.

Authorization: In this aspect, we check for the permissions that are given to a user or role. If a user is authorized to access a service, they are allowed to use it in the cloud environment.

456. What are the main cost factors of cloud based data center?

Costs in a Cloud based data center are different from a traditional data center. Main cost factors of cloud based data center are as follows:

Labor cost: We need skilled staff that can work with the cloud-based datacenter that we have selected for our operation. Since cloud is not a very old technology, it may get difficult to get the right skill people for handling cloud based datacenter.

Power cost: In some cloud operations, power costs are borne by the client. Since it is a variable cost, it can increase with the increase in scale and usage.

Computing cost: The biggest cost in Cloud environment is the cost that we pay to Cloud provider for giving us computing resources. This cost is much higher compared to the labor or power costs.

457. How can we measure the cloud-based services?

In a cloud-computing environment we pay for the services that we use. So main criteria to measure a cloud based service its usage.

For computing resource we measure by usage in terms of time and the power of computing resource.

For a storage resource we measure by usage in terms of bytes (giga bytes) and bandwidth used in data transfer.

Another important aspect of measuring a cloud service is its availability. A cloud provider has to specify the service level agreement (SLA) for the time for which service will be available in cloud.

458. How a traditional datacenter is different from a cloud environment?

In a traditional datacenter the cost of increasing the scale of computing environment is much higher than a Cloud computing environment. Also in a traditional data center, there are not much benefits of scaling down the operation when demand decreases. Since most of the expenditure is in capital spent of buying servers etc., scaling down just saves power cost, which is very less compared to other fixed costs.

Also in a Cloud environment there is no need to higher a large number of operations staff to maintain the datacenter. Cloud provider takes care of maintaining and upgrading the resources in Cloud environment.

With a traditional datacenter, people cost is very high since we have to hire a large number of technical operation people for in-house datacenter.

459. How will you optimize availability of your application in a Cloud environment?

In a Cloud environment, it is important to optimize the availability of an application by implementing disaster recovery strategy. For disaster recovery we create a backup application in another location of cloud environment. In case of complete failure at a data center we use the disaster recovery site to run the application.

Another aspect of cloud environment is that servers often fail or go down. In such a scenario it is important to implement the application in such a way that we just kill the slow server and restart another server to handle the traffic seamlessly.

460. What are the requirements for implementing IaaS strategy in Cloud?

Main requirements to implement IAAS are as follows:

Operating System (OS): We need an OS to support hypervisor in IaaS. We can use open source OS like Linux for this purpose.

Networking: We have to define and implement networking topology for IaaS implementation. We can use public or private network for this.

Cloud Model: We have to select the right cloud model for implementing IaaS strategy. It can be SaaS, PaaS or CaaS.