AWS Certified Cloud Practitioner

From Whizzlab & Summerized by – **JD**.

Note : Some points or topics may repeat or there might be minor spelling mistake or misplace.

1. Cloud : Simply The internet. more specifically, it's all of the things you can access remotely over the Internet. When something is in the **cloud**, it means it's stored on Internet servers instead of your computer's hard drive.
2. Cloud Computing : Ability to Harness the Power of Computing over the internet. Allows you to use a variety with little or no initial investment. Ability to create a virtual sever over internet. Pay for what you use.
3. AWS : Amazon Web Services. Its On-Demand cloud Computing Platform. Subsidiary of amazon. Largest Cloud Service Platform.
4. Region : A Region is a physical location in the world which consists of two or more Availability Zones (AZ's).
5. Availability Zone : An AZ is one or more discrete data centers, each with redundant power, networking and connectivity, housed in separate facilities. AWS is responsible for maintaining Datacenters. In Short An AZ is a collection of multiple physical Datacenters. When you write any resource in a data center it gets replicated to multiple data centers just to ensure data is made more available.
6. Edge Location : Edge Locations are endpoints for AWS which are used for caching content. Typically this consists of CloudFront, Amazon's Content Delivery Network (CDN)
7. S3 : Simple storage service : Flat Object Level Storage like Photos, etc which is static and does not change. Not meant for database or OS installations. Bucket is container to hold your object and then you can creating and upload object into buckets.

   7.1 Standard : Default class for bucket are accessed frequently.

   7.2 Reduced Redundancy : Used to store No critical data. Lower cost with reduced service level agreement.

   7.3 Standard IA and Onezone IA : Infrequently accessed Objects.

   7.4 Glacier and Deep Archive : For Data archival. Storage at much lower cost.

   Other features :

   7.5 Versioning : Have version of a single file for changes in object.

   7.6 S3 bucket as static website.

   7.7 Cross region Replication : To ensure objects are available in other regions. Disaster recovery or close to the user.

   7.9 Manage access to object using bucket policies.

8. Amazon Glacier : For storing or retaining data for longer period of time. You create a vault instead of bucket to hold the objects. In order to object you need AWS CLI or AWS SDK or lifecycle management. you have to submit a job request to retrieve an object and is known as standard retrieval. It could take 3-5 hours to download an object. With expedited retrieval which is at higher cost you can retrieve objects within minutes .
9. VPC or virtual Private Cloud : allows you to have isolated Virtual Network dedicated to your AWS account. It is isolated from other virtual networks defined in AWS. Once you have VPC you can

launch resources such as EC2 (Virtual Servers). Can have multiple VPC's Defined in AWS. When you create an AWS account, you get default VPC created per region. You can define Subnet in VPC which allows you to separate or provide boundaries for your resources.

10. EC2 : Elastic Compute Cloud Ability to create a virtual server on the cloud.
    Pricing Models :
    1. On-Demand : Most flexible pricing option. Not the most cheapest Option available.
    2. Spot Pricing : Run workloads on EC2 instances and also have upto 90% savings on cost. The instances are available based on spare capacity available in Aws. If the AWS runs out of capacity in that particular region then the copumte capacity will be taken away from you. You can decide either to hibernate, stop or terminate. Good if your workloads can be interrupted.
    3. Reserved Pricing : Pay an upfront and reserve an instance type. Save upto 75%.
       STANDARD RI : if you are sure of the type of workload that will run on the EC2 instance.
       CONVERTIBLE RI : This allows you to change the attributes of RI. But this is only possible if the result yields in RI of equal or greater value.
       SCHEDULED RI : Here you can launch instances during specific time windows.
    4. Dedicated Host : A Dedicated Host is a physical EC2 server dedicated for your use. Dedicated Hosts can help you reduce costs by allowing you to use your existing server-bound software licenses, including Windows Server, SQL Server, and SUSE Linux Enterprise Server (subject to your license terms), and can also help you meet compliance requirements.Can be purchased On-Demand (hourly). Can be purchased for up to 70% off.
11. Elastic Block Storage : Block Storage for EC2 Instances. There are different volume types available. You can have multiple volumes for an instance. You can enable Encryption for volumes. Create Snapshots of Volumes – these are known as EBS Snapshots. A Volume can be attached to any instance as long as the volume and instance are in the same availability zones.
    You can create different types of volumes :
    1. General purpose SSD : These are used for typical workloads such as webservers.
    2. Provisioned IOPS : This is for more resource intensive workloads such as database. Costs more than than General purpose SSD and that's because the added functionality of ability to handle the higher input and output operations.
    3. Throughput Optimized HDD : For workloads that need more throughput on the volume such as Big Data Applications.
    4. Cold HDD : Good for archive storage.
12. Costing in AWS :
    1. Pricing Calculator : Allows you to ge an indicative pricing on hosting resources in AWS. You don't need to have AWS account to use pricing calculator.
    2. Billing section : Can see the costs to date and the billing details.
    3. Cost Explorer : Allows you to analyse your spend. But you need to enable this in advance. After enabling it, it could take 24 hour to see the details In cost explorer. Forecast data available if you have enough data in your account. Your can create and save various reports for different departments. Cost Explorer has many features that allows you to drill down into the cost aspects based on different categories, Give you reports etc.
13. Benefits of moving to cloud : 1. Pay as you go. 2. No worry about insfrastructure 3. Best and new Cloud Services on AWS.

14. Service Continuity : Fault tolerance : ensuring that the services are available during any fault. High availability : If infrastructure goes down, you need to ensure the right measures are in place to ensure the application is still available.
    1. Availability Zones : Make use of availabiltity zones. Deploy EC2 instances across multiple availabity zones.
    2. Regions : For higher availability and for disaster recovery, deploy secondary solutions to multiple regions.
    3. Elastic load balancer : Make use of elastic load balancer for distributing traffic to your underlying EC2 instances.
15. AWS Organizations : Account management system. Manage all of your accounts. Get Consolidated Bills. The master account can get a consolidated bill for all member accounts. You can also get volume pricing discounts. You can also have service control policies at the organization level.
16. TCO Calculator : Total Cost of ownership calculator : Detailed comparison of the cost of your applications in an on premises or traditional hosting environment to AWS cloud.
17. Cost Allocation Tags : Tags are used to organize resources in AWS. Cost allocation Tags can be used to track resources at a detailed level from a costing aspect. Common use : When you want to have bills department wise or cost center wise. AWS-Generated Cost allocation tags : There are some inbuilt tags available with resources. User-Defined Cost Allocation Tags : Made my the user and the you need to activate it.
18. AWS Trusted Advisor : Recommendation Service to optimize performance and security. Looks at all AWS services that you are using and gives you Different types of recommedations.
19. Elastic Load Balancer : Used to distribute traffic to your underlying and backend virtual machines. Distribute requests to underlying EC2 instances or even AWS Lambda. It take sthe requests from the users and then equally distributes those to your backend servers or virtual machines. Completely Managed service you don't need to manage the different aspects of load balancer.
20. Auto Scaling : Used to scale your infrastructure/EC2 Instances based on demand. You can create autoscaling groups. You can create conditions for scaling process. Working :- 1. First define a launch configuration This defines the types of instances that needs to be a part of the autoscaling group. 2. You then define the autoscaling group. 3. For the scaling group, you can perform a manual scaling. 3. You can also perform a scheduled scaling. 4. You can also perform scaling based on metrics.
21. Route53 : Domain name system in AWS and also used for routing requests to resources hosted in AWS. Ability to register domain names. Also you can check the health of your resources. Traffic Routing Policy : 1. Simple routing policy : Used for routing traffic to a single resource. 2. Failover Routing Policy : Used for active passive Failover. 3. Geolocation Routing Policy : Route traffic based on the location of users. 4. Weighted Routing Policy : Route traffic to different resources on a weightage. 5. Latency Routing Policy : Route traffic to the region that provides the best latency.
22. Amazon Cloudfront : Content network distribution service. Used for effective distribution of content to users across the world. Distributes content with the help of edge locations and users receive content from the closest edge location. Process : 1. A user tries to access a webpage in your application. 2. The request is routed to the nearest edge location. 3. If the web content is in the cache of the edge location, it Is sent to the user. 4. If the web content is not present, the edge server makes a request to the origin. 5. As soon as the first bytes is received by the edge server, it starts sending the data to the user. 6. The data is ten cached for the further use.

23. Relational database : to host variety of database based on different types of service such as mySQL, Oracle, Microsoft SQL Server, marie DB, postgres SQL. Service that allows you to setup a relational database in AWS. A lot of administrative jobs are managed by AWS themselves. If you setup Relational database service with the AWS Relational database service, with the help of a wizard, it will deploy the MySQL solution for you on EC2 instance automatically. You can scale the underlying instance hosting the database instance at any point in time. Monitoring aspects are in place for the database instance via Cloudwatch service. You can enable automated backups. You can also create snapshots of your database at any point in time. Enable high availability of your database by using Multi-AZ feature (You have a primary database hosted in one availability zone and then the service will create secondary database in another availability zone and automatically this feature will do the synchronization of data from the primary to secondary database. So if the primary database fails, A switchover will occur to the secondary database)
24. DynamoDB : Fully managed NoSQL database. Provides better performance and better scalability. You don't need to manage any infrastructure. In DynamoDB, you directly start working with tables. In DynamoDB a table is a collection of items and each item is a collection of attributes. NoSQL data in DynamoDB is represented in .json. There are 2 different types of primary keys that are supported : 1. Simple Primary Key – partition key. Here the value of the attribute is sent to the internal hash function. That function decides where on the physical storage the item is stored. 2. Composite key – Consists of Partition key and Sort key. So if the items are stored on the same partition, you can then decide on another key which can be used to sort the items in the partition. Read and write Throughput - This is primary variable used to decide on the cost aspect for the table Here storage is not the prime cost variable. Read Throughput – Represented as Capacity Units. One Read Capacity Unity is one strongly consistent read request or two eventually consistent read requests, for an item up to 4KB in size Write Throughput – one write Capacity Unit is one write for an item up to 1KB in size. When not to use DynamoDB : 1. If you are going to perform complex queries on the data. 2. If you need to perform table joins.
25. AWS Lambda : Compute serverless service available in AWS. Here you don't need to maintain the infrastructure it Is managed by the service itself. Supports a host of programming languages such as Node.js, python, Ruby, Java, Go and .net. Working : 1. You have a code suppose .net code. 2. Deploy the code to AWS lambda. You can then run the code wherever you want. Here, infrastructure is maintained for you . You only get charged for the time the code runs.
26. AWS Elastic Beanstalk : Spin up environment in the least amount of time. Allows you to quickly deploy and manage applications in AWS. Here you don't need to worry about the underlying infrastructure. You can deploy different types of applications. 1. You submit the request to Elastic Beanstalk and it will create resources for you like EC2 instance it will automatically install the underlying application server and deploy your code, provision the load balancer and also provision your autoscaling group. Good when you want developers to have environment up and running quickly. Has support for a variety of programming languages – Go, Java, Node.js, PHP, Python. Also has support for application servers such as Tomcat and internet information services.
27. Simple Queue Service : Messaging Service in AWS. Hosted Queue service. Fully managed, secure and durable. Used to decouple components of a distributed applications
28. Simple Notification Service : Notification Service in AWS. Manages the delivery of messages. Different endpoints can subscribe to the simple Notification Service. Consumers can receive messages via different protocols. Working : 1. You create a topic. 2. You need to subscribe to the topic in order to receive the messages. 3. You can have multiple subscribers for a topic. 4. A

subscriber can be a lambda function, an HTTP/S endpoint, an SAS queue, email or SMS. 5. You can enable encryption at rest for the messages.

29. Cloudformation : Design or spin up resource/infrastructure in AWS via templates. Good way to control your infrastructure via code. The template will basically describe the resources you want to create in AWS and you can submit these template to Cloudformation and cloudformation service will deploy something called stack. You can use the same template to deploy multiple stack for multiple environment with similar configuration. The template is in Json or yaml format. Sections of template : 1. Resources – This defines the resources that need to be created. 2. Parameter : Send values to the template at runtime to make it more dynamic. 3. Output : if you want to store the output that can be reused.
30. Amazon Redshift : Data warehousing service in AWS. You can store petabytes of data using this service. Fully managed service. Redshift service is used to create a cluster of nodes that will be used to host the warehouse. Architecture - There is a leader node and under that there is a compute node. The Leader node Is responsible for taking the queries. The leader node then passes the queries to the compute Nodes. Here in Compute nides the queries are processed in parallel. Query Editor – You can use this inline query editor. But for that the nodes size need to be any of the following : DC1.8xlarge, DC2.large, DC2.8xlarge, DS2.8xlarge or you can download the SQL workbench via www.sql-workbench.eu . The SQL Workbench needs java as a prerequisite so ensure to have this package installed. You also need to download the amazon Redshift JDBC driver
31. Amazon Kinesis : Used to collect and process and analyse real-time data. Components that kinesis offer : 1. Kinesis Data streams – This is used for capturing real time data. A fully managed service. 2. Kinesis Video Streams – securely stream video from connected devices to AWS for analytics, Machine learning and other processing. 3. Kinesis Data Firehouse – capture, transform and load streams of data into AWS data stores. 4. Kinesis Data Analytics – process data streams in real time with SQL or java.
32. Amazon Aurora : This is available as a database engine with AWS relational database Service. Its compatible with MySQL and PostgreSQL. Delivers higher throughput than the traditional MySQL and PostgreSQL database engines.
33. Amazon ElastiCache : In- Memory Data store. Has 2 engines – Fully managed Redis and Memcached service. Fully managed and scalable service. Normally used for gaming type applications, IoT apps
34. Amazon EMR – Elastic Map Reduce : serverless service offered by AWS. Used to run Big Data frameworks such as Apache Hadoop and Apache Shark. Used to process and analyse large amount of data.
35. Shared Responsibility model : AWS is responsible for : 1. Underlying physical infrastructure. 2. Decommissioning of Old hardware. 3. Patching Firmware. 4. Data Center Security. Customer is responsible for : 1. Security Patching EC2 instances. 2 Encryption of data at rest. 3. Encryption of data in transit. 4. Looking after the costing aspects
36. Identity and access Management : Control access to resources/services into AWS. You can use in built policies or create new ones. Policies are used to control access or give permissions. Identities in IAM : 1. AWS root user – has full admin privileges to all service in AWS . 2. IAM user – Used to represent a person or user. 3. IAM group – Used to represent a group of users. 4. IAM Role – similar to an IAM user, but does not associate itself with any credentials. Policies in IAM : 1. Policies are used to control permissions. 2. Policies can be attached to users, groups or roles. 3. Policies can be assigned to resources as well. 4. You can use inbuilt policies or create your own custom policies according to requirements. Securing access in IAM : 1. Don’t use the root account for day by day activities. 2. Enable the MFA for privileged users. 3. Ensure users are

granted only the required privileges via policies – this is known as the least privilege. 4. You can also use password policies.

37. CloudWatch : Key monitoring service. Get metrics for various services you can create dashboards from various metrics. You can also create alarms – lets say you want IT admin staff to be alerted whenever CPU utilization for a resource goes beyond certain threshold. Can also be used to store logs. Can also create billing alarms. Also publish custom metrics. Cloudwatch logs - Services within AWS can store their logs in this service. You can also install agents to EC2 instances to send logs to AWS Cloudwatch logs. Cloudwatch Events – These can be used to connect to events triggered from AWS resources.
38. Cloud Trail : used for logging API calls onto AWS. Service used from a governance and compliance perspective. All actions taken in the AWS account are recorded by this service. Actions take from the console, CLI, SDK, API are recorded. It could be good security tool form an organization. It could answer questions like : Did any unauthorized access occur in my AWS account?, Did someone shutdown an EC2 instance?, Did someone launched an EC2 instance?, has someone logged on using the root account? Cloudtrail is automatically enabled as a service when the account is created the service records events which can be seen in an event history. This events get retained for 90 days. You can create a trail to retain more than 90 days or you want to do analysis on data. The trail can send events to an S3 bucket.
39. VPC and EC2 Security : when it comes to security for VPC there is something called Network Control Lists - The list is used to protect traffic into subnets hosted in a VPC. This gives you an extra layer of security at the subnet / network level. There are inbound and outbound rules that can be defined. Each rules can decide which protocol, port range and source to allow or deny traffic. Next you have Security Groups – These are associated with network interfaces attached to EC2 instances. Security groups can be used to decide what traffic can flow into and out of an EC2 instance. Like network control list, security groups also have inbound and outbound rules that can be defined. * Security groups are used at instance level to protect the traffic and Network Control lists are used at the subnet level *. Each rule can decide which protocol, port range and source to be used.
40. AWS web application Firewall : You can use the web application firewall along with the Application Load Balancer, Cloud fron distribution or the API gateway. You can create web access control lists to filter traffic that flows into your infrastructure. You can create rules to stop malicious traffic coming from specific IP addresses. You can create rules to stop traffic based on a header value in the incoming request.
41. AWS Shield : Can be used to protect against DDoS attacks. AWS Shield standard is given free for some of the AWS services. AWS Shield advanced which provides better support against DDoS attacks comes at an extra price.
42. AWS Artifact : you can use this service to download AWS security and compliance documents. If you want AWS ISO certifications or service organization control (SOC), Payment Card Industry (PCI) Reports, you can refer to the AWS Artifact Service. Submit these to auditors who need proof that of the security and compliance of the AWS infrastructure
43. AWS Rekognition : Service used to analyse videos and images. Can be used for face-based user verification. Also used to detect unsafe contents. Used to detect faces in images and stored videos. Can be used to search for faces in a container known as collection. Can be used to track the paths of people detected in a stored video. Can be used to detect text in images and convert it into machine-readable text. You can compare face in two pictures.
44. AWS OpsWorks : Configuration Management Service in AWS. Allows to enforce the desired state of your infrastructure. Allows you to integrate existing tools such as chef and puppet. If you want to automate the configuration of stack in AWS you would use OpsWorks.

45. AWS Certificates Manager : Service that is used to generate and manage public SSL/TLS certificates for AWS websites. This service has integration with other AWS services such as Elastic Load Balancer, amazon Cloudfront, elastic beanstalk. You can also import an existing certificate into ACM. You can't export public certificate to install on your individual sites or servers.
46. Personal Health Dashboard : Provides health events about the underlying AWS physical infrastructure. Issues by default are categorized into open issues, scheduled changes and other notifications. You can see all health events that pertain to your AWS account. You can see the details of each event. You can also setup notifications for the event via Cloudwatch Rules.
47. AWS QuickSight : Business intelligence cloud service. Used to create and publish interactive dashboards. You can give other users access to reports. You only pay for what you use. You first need to create a Quicksight account. If you are only one user, then you can use Quicksight for free. Here you are the author and the user. If you want to share reports with other users, you can create upto 4 users for free for 60 days. You need to define Data source to use quicksight – you can specify different sources from where to get your data. Data sources can be MySQL or Microsoft SQL server databases or can be existing AWS services such as AWS aurora, S3, Redshift. Spice- Next the data gets imported into SPICE. This is QuickSIght's in-memory optimized calculation engine. A free user gets 1 GB of SPICE data. And each paid user gets 10GB of SPICE data. Visualizations – Next you can start visualizing your data. Create Visualizations, dashboards. Create Quicksight account in the region where you have your resources.
48. AWS CodeDeploy : Deployments service in AWS. Can be used to automate deployments. You can automate deployments to EC2 instances, On-Premise instances, Lambda functions or Amazon ECS services.
49. Amazon Cognito : Service that provides authentication, authorization and user management for web and mobile applications. Users can use this service to either directly sign in with the username and password or user can use third party identity providers such as facebook or google. Components : 1. User pools – is made up of user directories. Used to perform signup and signin for application users. 2. Identity pools – Used to grant user access to AWS resources. Instead of developing modules for the sign-up and sign-in process, you can use Amazon Cognito. The in-built web-ui Is customizable. User directory management. Work with User profiles. Can use multifactor authentication.
50. Amazon Cloud9 : This is an integrated development environment which is available on AWS Cloud. You can access the IDE through the web browser itself. You can work with code in various programming languages such aa .net, go, python. You can also work with code associated with Lambda functions.
51. AWS X-Ray : service that is used to collect data about your requests. You can use this tool to optimise your application. You can use this for your applications or even AWS Lambda. It gives you an entire service map of your requests. It also gives you the average time spent for each request. You can see individual traces for your application. You can use the AWS X-Ray SDK to instrument your application. To use AWS X-ray from AWS Lambda, you have to enable it for your function. In AWS Lambda, by default the invocation time will be sent to AWS X-Ray. If you want to send information about other requests, you need to add instrumentation code.
52. CloudHSM : Provides hardware security modules on the cloud. These are the devices that can be used to process cryptographic operations. Provides secure storage for your cryptographic keys. CloudHSM is an important service when it comes to security. What can you do with CloudHSM – Generate, store, import, export and manage cryptographic keys, including symmetric and asymmetric key pairs. Use symmetric and asymmetric algorithms to encrypt and decrypt data. Cryptographically sign data. Generate cryptographically secure random data.

53. Cloud Service Models :
    1. IaaS : Infrastructure as a service : Here the underlying physical infrastructure is managed by AWS. A common example of IaaS is the AWS Elastic Compute Cloud service (EC2). Here you mange the instances, but you don't manage the underlying physical infrastructure. Here the clear advantage is that you don't have the burden to manage the physical infrastructure. It also helps to reduce capital costs – you don't need to invest in physical infrastructure. It also helps to reduce operational expenditure – you don't need to worry about adding servers, storage, cooling, networking.
    2. PaaS : Platform as a Service : Here the underlying physical infrastructure Is managed by AWS. Here even the virtualized environment is also managed by AWS. A common example of PaaS is the Amazon Relational Database Service (Amazon RDS). With this service, the time consuming activities of hardware, managing capacity, managing the virtual machines are managed by AWS. When it also comes to managing EC2 or underlying virtual hardware that is used for hosting databases that is also managed by the platform itself. This service also gives you high availability, fast performance, backup and restore features.
    3. SaaS : Software as a Service : Here the underlying physical infrastructure is managed by AWS. Here even the virtualised environment is also managed by AWS. And also the underlying software on the virtualized environment is managed by AWS if it is being hosted in AWS as such. Here the additional advantage is that you don't even have to manage the software as well. A common example of SaaS is an example of an Email service over here you just go and use the service itself.
54. Cloud Computing Deployment Models :
    1. Cloud Deployment Model : here all applications are deployed onto the cloud. Applications that would have been hosted in the on-premises environment can also migrated to the cloud. There are so many advantages of hosting your application on the cloud. You can save on costs. You don't have to invest on the physical hardware. You only pay for how much you use. You can use the latest services on the cloud.
    2. On-Premises Deployment Model : Here all applications are deployed onto your own data centers. No applications are deployed onto the cloud. Here the advantages is that you have complete control over the infrastructure. You also have complete control over the security aspect of your infrastructure. The disadvantage is that you need to invest in the infrastructure and security.
    3. Hybrid Deployment Model : Best of both Worlds. Here the applications are deployed both on your on-premises environment and also on your cloud environment. Here you can use the benefits of both environments. You can use services AWS Direct connect to connect both of your environments. You can save on costs for your cloud deployments. You can implement your own security protocols when it comes to your on-premises deployment.
55. Advantages on Cloud Computing : Six advantages of Cloud Computing –
    1. Trade Capital expense for variable expenses : Here you don't need to invest on hardware infrastructure. Instead on investing on data centers or servers, you only pay for how much you use so this becomes your variable expense.
    2. Benefits from massive economies of Scale : As more and more customers move to cloud, the costs of pay as you go can decrease.
    3. Stop guessing capacity : When companies need to deploy applications on their on-premises data centers, they need to decide aspects such as – how many servers does the application require?, How much storage does the company need to invest on?, if the

application starts to grow, how much should we invest on an on-going basis? When using the AWS Cloud, you don't need to worry on those aspects. You can spin up infrastructure whenever required. You can scale based on demand. You can terminate infrastructure when you don't require it.

4. Increase speed and agility : You don't have to make teams to wait before infrastructure is ready. With services such as AWS beanstalk you can create environments quickly for your development community. Creating EC2 instances just takes a few minutes. You can create databases also in a few minutes using relational database service (RDS).
5. Stop spending Money running and maintaining data centers : Apart from capital expenses on infrastructure, you can also incur operational expenses as well like Maintaining your servers, administration of the data center, maintaining cooling systems etc. all these need to be boned by the company but when it comes to AWS it is managed by the AWS itself.
6. Go Global in minutes.

56. More on Availability zones : Each region in the AWS Global infrastructure is made up of isolated locations known as Availability Zones. When you use a service such as AWS EC2, you can make use of Availability Zones. The usage of availability zones in AWS allows you to ensure higher availability for your overall system. If one availability zone goes down, you still have other availability zones in place.
57. Using IAM Roles : An IAM role is actually an identity in IAM that is created within your AWS account. The IAM role has specific permissions. The IAM role is not associated with a person. It does not have any long term credentials such as password associated with it so this is a more secure identity you can create in IAM. You can assume a role. When you assume a role, temporary security credentials are assigned for the role session. Different types of role : 1. AWS service role – here the role is allowed to perform actions in the account on your behalf. You can then use the role to access the desired service. 2. AWS service role for an EC2 instance - This is a special type of role that can be assigned to an EC2 instance. The role allows the EC2 instance to access other services in AWS. 3. AWS service-linked role - These role types are used by AWS services to access other AWS services. 4. Cross-account access – this allows access to resources in one account to a trusted principal in a different account.
58. Identity and access management – Best practices : Try never to use the AWS access keys which are assigned to the root account. If you do have the root access keys, delete the access keys. Don't share the AWS account root user password or the access keys with anyone. Create separate IAM users in your AWS account. You can group users together in IAM groups. When it comes to assigning permissions, assign permissions based on least privilege. Create custom managed policies for your permissions. Perform a regular review of user access. Perform a regular review of your custom managed policies. Configure a strong password for your users. Enable multi-factor Authentication for your users. Use roles wherever adequate. Rotate the credentials regularly when it comes to your users.
59. EC2 instances – Userdata and metadata :
    1. Instance Metadata : This is data about instance You can run commands on your EC2 instance to get data about the instance. The data is available via a local service that runs on https://169.254.169.254. There are 2 versions of instance metadata service that are available on EC2 instance.
    2. Instance Userdata : the user data for an EC2 instance can be used to run scripts on an EC2 instance when it is first launched. You can pass either shell scripts or cloud-init directives.
60. Elastic Container Service : This is a container management service. You can use this service to run, stop and manage containers. The containers run on a cluster. You can also schedule the

placement of the containers. The placement can be done based on resource needs, isolation policies and availability requirements. In Amazon ECS, you define the containers that need to run based on task definitions. AWS Fargate is a technology that is used along with amazon ECS. This can be used to run containers without having the need to manage servers or clusters.

61. AWS Lambda : This is a serverless compute service. Here you can run code without the need to provision or manage the underlying infrastructure. Also you only pay for the compute time you use. It supports a number of runtimes -Node.js, Python, Ruby, Java, .Net and Go. The underlying service will automatically scale the infrastructure based on demand.
62. AWS S3 Storage classes :
    1. Standard storage class : this is the default storage class assigned to an object. This is the idea storage class for objects that are accessed frequently. It delivers low latency and high throughput. It is resilient against events that could affect an entire Availability Zone. It is secure – has support for SSL for data transit at rest.
    2. Intelligent-Tiering class : here AWS S3 will move data to the most cost effective access tier. This would be based Amazon S3 monitoring the access patterns for an object. While monitoring there is no performance impact or operational overhead. This is ideal when there is unpredictable access patters for your data.
    3. Standard- Infrequent Access : This is ideal for data that is accesses less frequently. This type of storage is ideal for data requirements such as long term storage, backups. It delivers low latency and high throughput. It is resilient against events that could affect an entire Availability zone. It is secure – has support for SSL for data transit at rest. But here there is a small retrieval fee for the data. Hence this is ideal for data that is not accessed frequently.
    4. Zone-Infrequent access : here the difference is that data is stored in one availability zone. Hence the data storage costs are less than that of amazon S3 standard infrequent access. Ideal again for use cases for storing secondary backup copies of data. Again here you are charged for the data retrieval fee.
    5. S3 Glacier : This is a low cost storage option that is designed for data archiving. Here the service is built for high availability and durability. Here the data costs are much lower. But to retrieve data it can take time. The data retrieval could take between minutes and hours.
63. Elastic Block Storage Snapshots : you can use EBS Snapshots to take a backup of the data on your Amazon EBS Volumes. Here point in time snapshots are taken and stored in Amazon S3. You can then recreate an EBS Volume based on the Snapshot. Snapshots that are created out of encrypted volumes are automatically encrypted. Then the volumes created from encrypted snapshots are also encrypted.
64. Instance Store Volumes : This is storage that is located on the disks that are physically attached to the host computer. This Is ideal for storage that stores information that changes frequently – buffers and cache. The size of instance store depends on the instance type. You cant detach an instance store volume and then attach it to another instance. The data on the instance store only persists during the lifetime of the instance. The data on the instance store is lost during the following scenarios – The underlying disk drive fails, the instance stops, the instance hibernates, the instance terminates.
65. Elastic File System : This provides an elastic file system that can be used for AWS cloud services or on premises resources. It can grow and shrink automatically based on demand. It supports the network file systems. Multiple EC2 instances can access the EFS file system at the same time. Here you only pay for the storage that is used by the file system.
66. NAT instances and NAT Gateways : NAT – network address translation : can be used to enable instances in the private subnet to initiate outbound IPv4 traffic to the internet. The NAT instance is provisioned in the public subnet. The NAT instance needs to have internet access. There is a

special AMI available to create NAT instances. NAT Gateway – This is managed version of the NAT instance. Here you get a high available NAT service. It can scale up to 45Gbps. It is completely managed by AWS.

67. Public, private and Elastic IP addresses network interface for EC2:
    1. Private IP address : this is an IP address that Is not reachable over the internet. This is used for communication between instances in the same VPC. When you launch an instance in VPC, AWS automatically assigns a private IP address to the instance. This is selected from the IP address range that is available from the subnet.
    2. Public IP address : this is an IP address that is reachable from the internet. By default VPC, a public IP address is assigned to instance. But you can decide not to allocate a public IP address to the instance. A public IP address is assigned to the instance from Amazon's Pool of Public IPv4 addresses. The instance's public IP address is released when the instance is stopped, hibernated or terminated.
    3. Elastic IP address : If you don't want the public IP address to change, then use Elastic IP address. The Elastic IP address is static and does not change over time. You would create a new Elastic IP address and then assign it ti an instance. You can also disassociate an Elastic IP address from a resource and then associate it with a different resource.
68. AWS Storage Gateway : This service helps to connect an on premises software appliance with the cloud based storage. This helps to easily scale your storage with the use of AWS Cloud. There are different solutions available. 1. File gateway – this provides a file interface into S3. To use the file gateway, you first need to download a VM image for the gateway. Then you need to activate the file gateway. Once the gateway is activated, you can create and configure the file shares that are linked to the S3. The file shares can be accessed via the network file system (NFS) or Server message block(SMB) protocol. 2. Volume Gateway – this allows you to mount cloud based storage volumes using Internet Small Computer System Interface (iSCSI). Here you can either use cached or stored volumes. With Cached coleus, Amazon S2 is used as the primary data store. The frequently accessed data is cached locally on the storage gateway. With the stored volumes, the primary data is stored locally. The data is then backed up onto AWS. 3. Tape Gateway - This provides cloud based virtual tape storage. This service is used to provide a durable, cost-effective solution for archiving data onto AWS. Here you can use the virtual tape library to store data on virtual tape cartridges. The tape gateway is already preconfigured with a media changer and tape drives.
69. AWS VPN – Virtual Private Network or Virtual Network Connection - VPN is a general term. In AWS, you can use a VPN to connect your on premises data center onto AWS. You can create an AWS site-to-site VPN connection. Then all the traffic between the on premises data center and AWS would flow via the VPN connection. Components off a site-to-site VPN : 1. Virtual private gateway – this is the VPN concentrator on the Amazon side of the site-to-site VPN connection. 2. The virtual private gateway is attached to the VPC. 3. On the customer side you have a hardware or software decide that can route traffic on the internet. 4. You would create a customer gateway in AWS that would be used to represent the customer routing device.
70. AWS Direct Connect : this helps to connect your on premises data center to your AWS VPC. Here the connection is established over a standard Ethernet fibre-optic cable. Using the connection , you create virtual interfaces directly to AWS services.
71. AWS ElastiCache : This is a webservice that makes it easy to setup a distributed in-memory data store. It helps to provide a cached environment for your applications. It's a high performant, scalable and cost effective caching solution. There are two flavours of Amazon ElastiCache – Redis and Memcached.

1. Redis : Amazon ElastiCache for redis is a managed service for the Redis cache service. Here you get automatic detection and recovery from cache node failures. It also has support for replication of data onto a read-replica. It has support for authenticating users with role based access control.
2. Memcached : Amazon ElastiCache for Memcached is a managed service for the Memcached service. Choose Memcached if – you need a simple model possible for a caching solution. You need to run the cache on a large number of nides with multiple cores or threads. You need to scale out and scale in based on demand. Here the nodes can be added or removed from the cluster.

72. AWS Database Migration service : this is a cloud service that helps to migrate data between relational databases, data warehouses, NoSQL data stores and other data stores as well. You can also use data stores that are available in your on premises data centers. You can also perform on going replications in addition to one time migrations. It has support for source data stores that include oracle, Microsoft SQL server, MySQL, MariaDB, Azure SQL database. It has support for target data stores that include oracle, Microsoft SQL server, MySQL, Amazon RDS instance, amazon DynamoDB.
73. Personal and service Health Dashboard : This service can be used to learn about AWS health events that affect the AWS services or the AWS account. In the dashboard, you can see open issues and any notifications that occurred in the previous seven days. You also have an event log that displays the AWS health events that apply to the particular account. If there are any events, you can see details about the events. This service also integrates with AWS organizations and amazon Cloudwatch events.
74. AWS Config : this service provides a detailed view of the configuration of the AWS resources within your account. It would also show you how resources are related to one another. You can also see the past configuration of the resources. You can also see how the configuration and the relationships have changed over time. You can get a notification is required if a resource has been created, modified or deleted. You can also use AWS config rules to see if the configuration of resources drifts from what are the desired settings. Lets say you want to check if the rules in a security group are changing, then you can evaluate the configuration against those rules. All of the configuration data for the resources are sent to an Amazon S3 bucket.
75. AWS Key management service : This service allows you to create and control customer master keys. These keys can then be used to encrypt your data. This is a completely managed service. The AWS KMS customer managed keys are protected by hardware security modules. This service is also integrated with other AWS services as well. Concepts in Key management service : 1. Customer master key – this is a logical representation of master key. The CMK includes metadata which includes the Key ID, creation date, description and the key state. 2. AWS managed CMK – there are some services that use encryption keys to encrypt data. These are keys that are managed by AWS. You then use API's to generate data keys. You then encrypt the data with the data key.
76. Snowball devices : you can use the AWS Snowball service to transfer data between physical storage devices and the amazon S3. The snowball device is used for transferring large amount of data. It should be the preferred choice if you are transferring more than 10 TB of data. So the Snowball devise are physical devices. These are rugged devices. They are protected by the AWS Key management service. This helps to protect the data in transit. Here the company does not need to buy or maintain their own hardware devices. The snowball device is its own shipping container. With snowball device, you can import and export data into Amazon S3. With Snowball edge, you have the following additional features. You get durable local storage, local compute with AWS Lambda, you can use it in a cluster of devices.

Process :

1. You create a job in the AWS Snow family Management console.
2. Then the snowball device is sent to the customer.
3. Then transfer the data onto the device.
4. Then ship the container back to AWS.
5. AWS will then transfer the data onto Amazon S3.

77. Amazon GuardDuty : This is a cloud service from AWS that monitors and analyses processes from the data sources that include VPC Flow Logs, AWS CloudTrail management event logs, Cloudtrail S3 data event logs and DNS logs. It uses its own intelligent feeds and machine learning algorithms to determine threats based on the analysed data. For example, it help detect compromised EC2 instances.
78. Amazon Marcie : This is a fully managed security and data privacy service. This service makes use of machine learning and pattern matching to help discover, monitor and protect sensitive data in AWS. It helps to perform discovery of sensitive data such as personally identifiable information (PII) and financial data. Hence it helps to give better understanding of data that is stored in S3. And also help detect potential issues with the security or privacy of data.
79. AWS Inspector : this service helps to inspect the security state of applications on EC2 instances.. it also helps to test the network accessibility of the Amazon EC2 instances. This service performs an assessment and checks for vulnerabilities based on best practices. After the assessment is complete, you get a detailed list of security findings.