Classic Solutions Architecture Q&A Points –

Q1. Your website TriangleSunglasses.com is hosted on a fleet of EC2 instances managed by an Auto Scaling Group and fronted by an Application Load Balancer. Your ASG has been configured to scale on-demand based on the traffic going to your website. To reduce costs, you have configured the ASG to scale based on the traffic going through the ALB. To make the solution highly available, you have updated your ASG and set the minimum capacity to 2. How can you further reduce the costs while respecting the requirements?

1. Reserve the 2 EC2 instances. This is the way to save further costs as we will run 2 EC2 instances no matter what.

Q2. Which of the following will NOT help us while designing a STATELESS application tier?

1. EBS volumes are created in a specific AZ and can only be attached to one EC2 instance at a time.

Q3. You want to install software updates on 100s of Linux EC2 instances that you manage. You want to store these updates on shared storage which should be dynamically loaded on the EC2 instances and shouldn't require heavy operations. What do you suggest?

1. Store the software update in EFS and mount EFS as a network drive at startup.

EFS is a network file system (NFS) that allows you to mount the same file system to 100s of EC2 instances. Storing software updates on an EFS allows each EC2 instance to access them.

Q4. As a Solutions Architect, you're planning to migrate a complex ERP software suite to AWS Cloud. You're planning to host the software on a set of Linux EC2 instances managed by an Auto Scaling Group. The software traditionally takes over an hour to set up on a Linux machine. How do you recommend you speed up the installation process when there's a scale-out event?

1. Use Golden AMI, Golden AMI is an image that contains all your software installed and configured so that future EC2 instances can boot up quickly from that AMI.

Q5. You're developing an application and would like to deploy it to Elastic Beanstalk with minimal cost. You should run it in ..................

1. The question mentions that you're still in the development stage and you want to reduce costs. Single Instance Mode will create one EC2 instance and one Elastic IP.

Q6. You're deploying your application to an Elastic Beanstalk environment but you notice that the deployment process is painfully slow. After reviewing the logs, you found that your dependencies are resolved on each EC2 instance each time you deploy. How can you speed up the deployment process with minimal impact?

1. Create a Golden AMI that contains all the dependencies and use that image to launch the EC2 instances.

S3 Bucket Q&A Points –

Q1. You have a 25 GB file that you're trying to upload to S3 but you're getting errors. What is a possible solution for this?

1. Multi-Part Upload is recommended as soon as the file is over 5GB.

Q2. You're getting errors while trying to create a new S3 bucket named "dev". You're using a new AWS Account with no S3 buckets created before. What is a possible cause for this?

1. S3 bucket names must be globally unique and ‘dev’ is already taken.

Q3. You have enabled versioning in your S3 bucket which already contains a lot of files. Which version will the existing files have?

1. Null

Q4. You have updated an S3 bucket policy to allow IAM users to read/write files in the S3 bucket, but one of the users complain that he can't perform a PutObject API call. What is a possible cause for this?

1. The IAM user must have an explicit DENY in the attached IAM policy.

Q5. You want the content of an S3 bucket to be fully available in different AWS Regions. That will help your team perform data analysis at the lowest latency and cost possible. What S3 feature should you use?

1. S3 Replication allows you to replicate data from an S3 bucket to another in the same/different AWS Region.

Q6. You have 3 S3 buckets. One source bucket A, and two destination buckets B and C in different AWS Regions. You want to replicate objects from bucket A to both bucket B and C. How would you achieve this?

1. Configure Replication A -> B and then again A -> C

Q7. Which of the following is NOT a Glacier Deep Archive retrieval mode?

1. Expedited

Q1. You have an S3 bucket that has S3 Versioning enabled. This S3 bucket has a lot of objects, and you would like to remove old object versions to reduce costs. What's the best approach to automate the deletion of these old object versions?

1. S3 Lifecycle Rules – Expiration Actions

Q2. How can you automate the transition of S3 objects between their different tiers?

1. S3 Lifecycle Rules

Q3. While you're uploading large files to an S3 bucket using Multi-part Upload, there are a lot of unfinished parts stored in the S3 bucket due to network issues. You are not using these unfinished parts and they cost you money. What is the best approach to remove these unfinished parts?

1. Use an S3 Lifecycle Policy to automate old/unfinished parts deletion.

Q4. You are looking to get recommendations for S3 Lifecycle Rules. How can you analyze the optimal number of days to move objects between different storage tiers?

1. S3 Analytics

Q5. You are looking to build an index of your files in S3, using Amazon RDS PostgreSQL. To build this index, it is necessary to read the first 250 bytes of each object in S3, which contains some metadata about the content of the file itself. There are over 100,000 files in your S3 bucket, amounting to 50 TB of data. How can you build this index efficiently?

1. Create an application that will traverse the S3 bucket, issue a Byte Range Fetch for the first 250 bytes, and store that information in RDS.

Q6. You have a large dataset stored on-premises that you want to upload to the S3 bucket. The dataset is divided into 10 GB files. You have good bandwidth but your Internet connection isn't stable. What is the best way to upload this dataset to S3 and ensure that the process is fast and avoid any problems with the Internet connection?

1. Using S3 Multi-Part Upload & S3 Transfer Acceleration

Q7. You would like to retrieve a subset of your dataset stored in S3 with the .csv format. You would like to retrieve a month of data and only 3 columns out of 10, to minimize compute and network costs. What should you use?

1. S3 Select

Q8. A company is preparing for compliance and regulatory review on its infrastructure on AWS. Currently, they have their files stored on S3 buckets that are not encrypted, which must be encrypted as required for compliance and regulatory review. Which S3 feature allows them to encrypt all files in their S3 buckets in the most efficient and cost-effective way?

1. S3 Batch Operations

AWS S3 Security Q&A Points –

Q1. Your client wants to make sure that file encryption is happening in S3, but he wants to fully manage the encryption keys and never store them in AWS. You recommend him to use ->

1. SSE-C

Q2. A company you're working for wants their data stored in S3 to be encrypted. They don't mind the encryption keys stored and managed by AWS, but they want to maintain control over the rotation policy of the encryption keys. You recommend them to use ->

1. With SSE-KMS, the encryption happens in AWS, and the encryption keys are managed by AWS but you have full control over the rotation policy of the encryption key. Encryption keys stored in AWS.

Q3. Your company does not trust AWS for the encryption process and wants it to happen on the application. You recommend them to use

1. With Client-Side Encryption, you must do the encryption yourself and you have full control over the encryption keys. You perform the encryption yourself and send the encrypted data to AWS. AWS does not know your encryption keys and cannot decrypt your data.

Q4. You have a website that loads files from an S3 bucket. When you try the URL of the files directly in your Chrome browser it works, but when a website with a different domain tries to load these files it doesn't. What's the problem?

1. Cross-Origin Resource Sharing (CORS) defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. To learn more about CORS, go here: <https://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html>

Q5. An e-commerce company has its customers and orders data stored in an S3 bucket. The company’s CEO wants to generate a report to show the list of customers and the revenue for each customer. Customer data stored in files on the S3 bucket has sensitive information that we don’t want to expose in the report. How do you recommend the report can be created without exposing sensitive information?

1. Use S3 Object Lambda to change the objects before they are retrieved by the report generator application.

Q6. You suspect that some of your employees try to access files in an S3 bucket that they don't have access to. How can you verify this is indeed the case without them noticing?

1. S3 Access Logs log all the requests made to S3 buckets and Amazon Athena can then be used to run serverless analytics on top of the log files.

Q7. You are looking to provide temporary URLs to a growing list of federated users to allow them to perform a file upload on your S3 bucket to a specific location. What should you use?

1. S3 Pre-Signed URLs are temporary URLs that you generate to grant time-limited access to some actions in your S3 bucket.

Q8. For compliance reasons, your company has a policy mandate that database backups must be retained for 4 years. It shouldn't be possible to erase them. What do you recommend?

1. Glacier Vaults with Vault Lock Policies

Q9. You would like all your files in an S3 bucket to be encrypted by default. What is the optimal way of achieving this?

1. By default encryption is enabled.

Q10. You have enabled versioning and want to be extra careful when it comes to deleting files on an S3 bucket. What should you enable to prevent accidental permanent deletions?

1. MFA Delete forces users to use MFA codes before deleting S3 objects. It's an extra level of security to prevent accidental deletions.

Q11. A company has its data and files stored on some S3 buckets. Some of these files need to be kept for a predefined period of time and protected from being overwritten and deletion according to company compliance policy. Which S3 feature helps you in doing this?

1. S3 Object Lock – Retention Compliance Mode

Q12. Which of the following S3 Object Lock configuration allows you to prevent an object or its versions from being overwritten or deleted indefinitely and gives you the ability to remove it manually?

1. Legal hold.

CloudFront and AWS Global Accelerator and Q&A Points –

Q1. You have a CloudFront Distribution that serves your website hosted on a fleet of EC2 instances behind an Application Load Balancer. All your clients are from the United States, but you found that some malicious requests are coming from other countries. What should you do to only allow users from the US and block other countries.

1. Using CloudFront Geo Restriction

Q2. You have a static website hosted on an S3 bucket. You have created a CloudFront Distribution that points to your S3 bucket to better serve your requests and improve performance. After a while, you noticed that users can still access your website directly from the S3 bucket. You want to enforce users to access the website only through CloudFront. How would you achieve that?

1. Configuring a CloudFront Distribution and create an Origin Access Control (OAC), then update your S3 Bucket Policy to only accept requests from your CloudFront Distribution.

Q3. What does this S3 bucket policy do?

{

    "Version": "2012-10-17",

    "Id": "Mystery policy",

    "Statement": [{

        "Sid": "What could it be?",

        "Effect": "Allow",

        "Principal": {

           "Service": "cloudfront.amazonaws.com"

        },

        "Action": "s3:GetObject",

        "Resource": "arn:aws:s3:::examplebucket/\*",  
        "Condition": {  
            "StringEquals": {  
                "AWS:SourceArn": "arn:aws:cloudfront::123456789012:distribution/EDFDVBD6EXAMPLE"  
            }  
        }

    }]

}

1. This only allows the S3 bucket content to be accessed from your CloudFront Distribution.

Q4. A WordPress website is hosted in a set of EC2 instances in an EC2 Auto Scaling Group and fronted by a CloudFront Distribution which is configured to cache the content for 3 days. You have released a new version of the website and want to release it immediately to production without waiting for 3 days for the cached content to be expired. What is the easiest and most efficient way to solve this?

1. CloudFront Cache Invalidation

Q5. A company is deploying a media-sharing website to AWS. They are going to use CloudFront to deliver the content with low latency to their customers where they are located in both US and Europe only. After a while there a huge cost for CloudFront. Which CloudFront feature allows you to decrease costs by targeting only US and Europe?

1. CloudFront Price Classes

Q6. A company is migrating a web application to AWS Cloud and they are going to use a set of EC2 instances in an EC2 Auto Scaling Group. The web application is made of multiple components so they will need a host-based routing feature to route to specific web application components. This web application is used by many customers and therefore the web application must have a static IP address so it can be whitelisted by the customers’ firewalls. As the customers are distributed around the world, the web application must also provide low latency to all customers. Which AWS service can help you to assign a static IP address and provide low latency across the globe?

1. AWS Global Accelerator + Application Load Balancer

AWS Storage Extras Q&A Points –

Q1. You need to move hundreds of Terabytes into Amazon S3, then process the data using a fleet of EC2 instances. You have a 1 Gbit/s broadband. You would like to move the data faster and possibly processing it while in transit. What do you recommend?

1. Snowball Edge is the right answer as it comes with computing capabilities and allows you to pre-process the data while it's being moved into Snowball.

Q2. You want to expose virtually infinite storage for your tape backups. You want to keep the same software you're using and want an iSCSI compatible interface. What do you use?

1. AWS Storage Gateway – Tape Gateway

Q3. Your EC2 Windows Servers need to share some data by having a Network File System mounted on them which respects the Windows security mechanisms and has integration with Microsoft Active Directory. What do you recommend?

1. Amazon FSx for Windows (File Server)

Q4. You have hundreds of Terabytes that you want to migrate to AWS S3 as soon as possible. You tried to use your network bandwidth and it will take around 3 weeks to complete the upload process. What is the recommended approach to using in this situation?

1. AWS Snowball Edge

Q5. You have a large dataset stored in S3 that you want to access from on-premises servers using the NFS or SMB protocol. Also, you want to authenticate access to these files through on-premises Microsoft AD. What would you use?

1. AWS Storage Gateway – S3 File Gateway

Q6. You are planning to migrate your company's infrastructure from on-premises to AWS Cloud. You have an on-premises Microsoft Windows File Server that you want to migrate. What is the most suitable AWS service you can use?

1. Amazon FSx for Windows (File Server)

Q7. You would like to have a distributed POSIX compliant file system that will allow you to maximize the IOPS in order to perform some High-Performance Computing (HPC) and genomics computational research. This file system has to easily scale to millions of IOPS. What do you recommend?

1. Amazon FSx for Lustre

Q8. Which deployment option in the FSx file system provides you with long-term storage that's replicated within AZ?

1. Persistent File System - Provides long-term storage where data is replicated within the same AZ. Failed files were replaced within minutes.

Q9. Which of the following protocols is NOT supported by AWS Transfer Family?

1. Transport Layer Security (TLS), AWS Transfer Family is a managed service for file transfers into and out of S3 or EFS using the FTP protocol, thus TLS is not supported.

Q10. A company uses a lot of files and data which is stored in an FSx for Windows File Server storage on AWS. Those files are currently used by the resources hosted on AWS. There’s a requirement for those files to be accessed on-premises with low latency. Which AWS service can help you achieve this?

1. FSx File Gateway

Q11. A Solutions Architect is working on planning the migration of a startup company from on-premises to AWS. Currently, their infrastructure consists of many servers and 30 TB of data hosted on a shared NFS storage. He has decided to use Amazon S3 to host the data. Which AWS service can efficiently migrate the data from on-premises to S3?

1. AWS DataSync

Q12. Which AWS service is best suited to migrate a large amount of data from an S3 bucket to an EFS file system?

1. AWS DataSync

Q13. A Machine Learning company is working on a set of datasets that are hosted on S3 buckets. The company decided to release those datasets to the public to be useful for others in their research, but they don’t want to configure the S3 bucket to be public. And those datasets should be exposed over the FTP protocol. What can they do to do the requirement efficiently and with the least effort?

1. Use AWS Transfer Family

Q14. Amazon FSx for NetApp ONTAP is compatible with the NFS, SMB and iSCSI protocols, except FTP

Q15. Which AWS service is best suited when migrating from an on-premises ZFS file system to AWS?

1. Amazon FSx for OpenZFS

Q16. A company is running Amazon S3 File Gateway to host their data on S3 buckets and is able to mount them on-premises using SMB. The data currently is hosted on S3 Standard storage class and there is a requirement to reduce the costs for S3. So, they have decided to migrate some of those data to S3 Glacier. What is the most efficient way they can use to move the data to S3 Glacier automatically?

1. Using S3 Lifecycle Policy

Q17. You have on-premises sensitive files and documents that you want to regularly synchronize to AWS to keep another copy. Which AWS service can help you with that?

1. AWS DataSync is an online data transfer service that simplifies, automates, and accelerates moving data between on-premises storage systems and AWS Storage services, as well as between AWS Storage services.

Messaging and Integration Q&A Points –

Decoupling Applications SQS, SNS and Kinesis –

Q1. You have an e-commerce website, and you are preparing for Black Friday which is the biggest sale of the year. You expect that your traffic will increase by 100x. Your website already using an SQS Standard Queue, and you're running a fleet of EC2 instances in an Auto Scaling Group to consume SQS messages. What should you do to prepare your SQS Queue?

1. Nothing is required as SQS scales automatically.

Q2. You have an SQS Queue where each consumer polls 10 messages at a time and finishes processing them in 1 minute. After a while, you noticed that the same SQS messages are received by different consumers resulting in your messages being processed more than once. What should you do to resolve this issue?

1. Increase the visibility timeout. SQS Visibility Timeout is a period during which Amazon SQS prevents other consumers from receiving and processing the message again. In Visibility Timeout, a message is hidden only after it is consumed from the queue. Increasing the Visibility Timeout gives more time to the consumer to process the message and prevent duplicate reading of the message. (Default: 30 sec., min.: 0 sec., max.: 12 hours)

Q3. Which SQS Queue type allows your messages to be processed exactly once and in order?

1. SQS FIFO (First-In-First-Out) Queues have all the capabilities of the SQS Standard Queue, plus the following two features. First, the order in which messages are sent and received are strictly preserved and a message is delivered once and remains available until a consumer process and deletes it. Second, duplicated messages are not introduced into the queue.

Q4. You have 3 different applications that you'd like to send them the same message. All 3 applications are using SQS. What is the best approach would you choose?

1. Using SNS+SQS Fan Out Pattern, this is a common pattern where only one message is sent to the SNS topic and then "fan-out" to multiple SQS queues. This approach has the following features: it's fully decoupled, no data loss, and you can add more SQS queues (more applications) over time.

Q5. You have a Kinesis data stream with 6 shards provisioned. This data stream usually receiving 5 MB/s of data and sending out 8 MB/s. Occasionally, your traffic spikes up to 2x and you get a ProvisionedThroughputExceeded exception. What should you do to resolve the issue?

1. Add more Shards.

The capacity limits of a Kinesis data stream are defined by the number of shards within the data stream. The limits can be exceeded by either data throughput or the number of reading data calls. Each shard allows for 1 MB/s incoming data and 2 MB/s outgoing data. You should increase the number of shards within your data stream to provide enough capacity.

Q6. You have a website where you want to analyze clickstream data such as the sequence of clicks a user makes, the amount of time a user spends, and where the navigation begins and how it ends. You decided to use Amazon Kinesis, so you have configured the website to send these clickstream data all the way to a Kinesis data stream. While you checking the data sent to your Kinesis data stream, you found that the users' data is not ordered and the data for one individual user is spread across many shards. How would you fix this problem?

1. For each record sent to Kinesis add a partition key that represents the identity of the user.

Kinesis Data Stream uses the partition key associated with each data record to determine which shard a given data record belongs to. When you use the identity of each user as the partition key, this ensures the data for each user is ordered hence sent to the same shard.

Q7. You are running an application that produces a large amount of real-time data that you want to load into S3 and Redshift. Also, these data need to be transformed before being delivered to their destination. What is the best architecture would you choose?

1. Kinesis Data Streams + Kinesis Data Firehose

This is a perfect combo of technology for loading data near real-time data into S3 and Redshift. Kinesis Data Firehose supports custom data transformations using AWS Lambda.

Q8. Which of the following is NOT a supported subscriber for AWS SNS?

1. Kinesis Data Firehose is now supported, but not Kinesis Data Streams.

Q9. Which AWS service helps you when you want to send email notifications to your users?

1. Amazon SNS

Q10. You're running many micro-services applications on-premises and they communicate using a message broker that supports MQTT protocol. You're planning to migrate these applications to AWS without re-engineering the applications and modifying the code. Which AWS service allows you to get a managed message broker that supports the MQTT protocol?

1. Amazon MQ supports industry-standard APIs such as JMS and NMS, and protocols for messaging, including AMQP, STOMP, MQTT, and WebSocket.

Q11. An e-commerce company is preparing for a big marketing promotion that will bring millions of transactions. Their website is hosted on EC2 instances in an Auto Scaling Group and they are using Amazon Aurora as their database. The Aurora database has a bottleneck and a lot of transactions have been failed in the last promotion they have made as they had a lot of transaction and the Aurora database wasn’t prepared to handle these too many transactions. What do you recommend to handle those transactions and prevent any failed transactions?

1. Use SQS as a buffer to write to Aurora

Q12. A company is using Amazon Kinesis Data Streams to ingest clickstream data and then do some analytical processes on it. There is a campaign in the next few days and the traffic is unpredictable which might grow up to 100x. What Kinesis Data Stream capacity mode do you recommend?

1. On-demand Mode

Containers on AWS Q&A Points – ECS, Docker, EKS

Q1. You have multiple Docker-based applications hosted on-premises that you want to migrate to AWS. You don't want to provision or manage any infrastructure; you just want to run your containers on AWS. Which AWS service should you choose?

1. AWS Fargate allows you to run your containers on AWS without managing any servers.

Q2. Amazon Elastic Container Service (ECS) has two Launch Types: .................. and ..................

1. Amazon EC2 Launch Type and Fargate Launch Type

Q3. You have an application hosted on an ECS Cluster (EC2 Launch Type) where you want your ECS tasks to upload files to an S3 bucket. Which IAM Role for your ECS Tasks should you modify?

1. ECS Task Role is the IAM Role used by the ECS task itself. Use when your container wants to call other AWS services like S3, SQS, etc.

Q4. You're planning to migrate a WordPress website running on Docker containers from on-premises to AWS. You have decided to run the application in an ECS Cluster, but you want your docker containers to access the same WordPress website content such as website files, images, videos, etc. What do you recommend achieving this?

1. Mount an EFS Volume.

EFS volume can be shared between different EC2 instances and different ECS Tasks. It can be used as a persistent multi-AZ shared storage for your containers.

Q5. You are deploying an application on an ECS Cluster made of EC2 instances. Currently, the cluster is hosting one application that is issuing API calls to DynamoDB successfully. Upon adding a second application, which issues API calls to S3, you are getting authorization issues. What should you do to resolve the problem and ensure proper security?

1. Create an IAM task for the new application.

Q6. You are migrating your on-premises Docker-based applications to Amazon ECS. You were using Docker Hub Container Image Library as your container image repository. Which is an alternative AWS service which is fully integrated with Amazon ECS?

1. ECR. Amazon ECR is a fully managed container registry that makes it easy to store, manage, share, and deploy your container images. ECR is fully integrated with Amazon ECS, allowing easy retrieval of container images from ECR while managing and running containers using ECS.

Q7. Amazon EKS supports the following node types, EXCEPT ………………..

1. It doesn’t support AWS Lambda node type.

Q8. A developer has a running website and APIs on his local machine using containers and he wants to deploy both of them on AWS. The developer is new to AWS and doesn’t know much about different AWS services. Which of the following AWS services allows the developer to build and deploy the website and the APIs in the easiest way according to AWS best practices?

1. AWS App Runner

Serverless on AWS – Lambda, DynamoDB, API Gateway Q&A Points –

Q2. Before you create a DynamoDB table, you need to provision the EC2 instance the DynamoDB table will be running on.

1. False,

DynamoDB is serverless with no servers to provision, patch, or manage and no software to install, maintain or operate. It automatically scales tables up and down to adjust for capacity and maintain performance. It provides both provisioned (specify RCU & WCU) and on-demand (pay for what you use) capacity modes.

Q3. You have provisioned a DynamoDB table with 10 RCUs and 10 WCUs. A month later you want to increase the RCU to handle more read traffic. What should you do?

1. Can increase RCU and keep WCU the same,

RCU and WCU are decoupled, so you can increase/decrease each value separately.

Q4. You have an e-commerce website where you are using DynamoDB as your database. You are about to enter the Christmas sale and you have a few items which are very popular, and you expect that they will be read often. Unfortunately, last year due to the huge traffic you had the ProvisionedThroughputExceededException exception. What would you do to prevent this error from happening again?

1. Create a DAX cluster.

DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for DynamoDB that delivers up to 10x performance improvement. It caches the most frequently used data, thus offloading the heavy reads on hot keys off your DynamoDB table, hence preventing the "ProvisionedThroughputExceededException" exception.

Q5. You have developed a mobile application that uses DynamoDB as its datastore. You want to automate sending welcome emails to new users after they sign up. What is the most efficient way to achieve this?

1. Enable DynamoDB Stream

DynamoDB Streams allows you to capture a time-ordered sequence of item-level modifications in a DynamoDB table. It's integrated with AWS Lambda so that you create triggers that automatically respond to events in real-time.

Q6. To create a serverless API, you should integrate Amazon API Gateway with ......................

1. AWS Lambda

Q7. When you are using an Edge-Optimized API Gateway, your API Gateway lives in CloudFront Edge Locations across all AWS Regions.

1. False,

An Edge-Optimized API Gateway is best for geographically distributed clients. API requests are routed to the nearest CloudFront Edge Location which improves latency. The API Gateway still lives in one AWS Region.

Q8. You are running an application in production that is leveraging DynamoDB as its datastore and is experiencing smooth sustained usage. There is a need to make the application run in development mode as well, where it will experience the unpredictable volume of requests. What is the most cost-effective solution that you recommend?

1. Use Provisioned Capacity Mode with Auto Scaling enabled for production and use On-Demand Capacity Mode for development.

Q9. You have an application that is served globally using CloudFront Distribution. You want to authenticate users at the CloudFront Edge Locations instead of authentication requests go all the way to your origins. What should you use to satisfy this requirement?

1. Lambda@Edge is a feature of CloudFront that lets you run code closer to your users, which improves performance and reduces latency.

Q10. The maximum size of an item in a DynamoDB table is ...................

1. 400KB

Q11. Which AWS service allows you to build Serverless workflows using AWS services (e.g., Lambda) and supports human approval?

1. AWS Step Functions

Q12. A company has a serverless application on AWS which consists of Lambda, DynamoDB, and Step Functions. In the last month, there are an increase in the number of requests against the application which results in an increase in DynamoDB costs, and requests started to be throttled. After further investigation, it shows that the majority of requests are read requests against some queries in the DynamoDB table. What do you recommend preventing throttles and reduce costs efficiently?

1. Use DynamoDB Accelerator (DAX) to cache the most requested read data.

Q13. You are a DevOps engineer in a football company that has a website that is backed by a DynamoDB table. The table stores viewers’ feedback for football matches. You have been tasked to work with the analytics team to generate reports on the viewers’ feedback. The analytics team wants the data in DynamoDB in json format and hosted in an S3 bucket to start working on it and create the reports. What is the best and most cost-effective way to convert DynamoDB data to json files?

1. Select DynamoDB table then select Export to S3

Q14. A website is currently in the development process and it is going to be hosted on AWS. There is a requirement to store user sessions for users logged in to the website with an automatic expiry and deletion of expired user sessions. Which of the following AWS services are best suited for this use case?

1. Store users’ sessions in a DynamoDB table and enable TTL

Q15. You have a mobile application and would like to give your users access to their own personal space in the S3 bucket. How do you achieve that?

1. Use Amazon Cognito Identity Federation

Amazon Cognito can be used to federate mobile user accounts and provide them with their own IAM permissions, so they can be able to access their own personal space in the S3 bucket.

Q16. You are developing a new web and mobile application that will be hosted on AWS and currently, you are working on developing the login and signup page. The application backend is serverless and you are using Lambda, DynamoDB, and API Gateway. Which of the following is the best and easiest approach to configure the authentication for your backend?

1. Use Cognito User Pools

Q17. You are running a mobile application where you want each registered user to upload/download images to/from his own folder in the S3 bucket. Also, you want to give your users to sign-up and sign in using their social media accounts (e.g., Facebook). Which AWS service should you choose?

1. Amazon Cognito

Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. Amazon Cognito scales to millions of users and supports sign-in with social identity providers, such as Apple, Facebook, Google, and Amazon, and enterprise identity providers via SAML 2.0 and OpenID Connect.

Serverless Solutions Architectures on AWS – Q&A Points –

Q1. A startup company plans to run its application on AWS. As a solutions architect, the company hired you to design and implement a fully Serverless REST API. Which technology stack do you recommend?

1. API Gateway + AWS Lambda

Q2. The following AWS services have an out of the box caching feature, EXCEPT .................

1. Lambda does not have an out-of-the-box caching feature.

Q3. You have a lot of static files stored in an S3 bucket that you want to distribute globally to your users. Which AWS service should you use?

1. Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds. This is a perfect use case for Amazon CloudFront.

Q4. You have created a DynamoDB table in ap-northeast-1 and would like to make it available in eu-west-1, so you decided to create a DynamoDB Global Table. What needs to be enabled first before you create a DynamoDB Global Table?

1. DynamoDB Streams enable DynamoDB to get a changelog and use that changelog to replicate data across replica tables in other AWS Regions.

Q5. You have configured a Lambda function to run each time an item is added to a DynamoDB table using DynamoDB Streams. The function is meant to insert messages into the SQS queue for further long processing jobs. Each time the Lambda function is invoked, it seems able to read from the DynamoDB Stream but it isn't able to insert the messages into the SQS queue. What do you think the problem is?

1. The Lambda Execution IAM Role is missing permissions.

Q6. You would like to create an architecture for a micro-services application whose sole purpose is to encode videos stored in an S3 bucket and store the encoded videos back into an S3 bucket. You would like to make this micro-services application reliable and has the ability to retry upon failures. Each video may take over 25 minutes to be processed. The services used in the architecture should be asynchronous and should have the capability to be stopped for a day and resume the next day from the videos that haven't been encoded yet. Which of the following AWS services would you recommend in this scenario?

1. Amazon SQS + Amazon EC2 - Amazon SQS allows you to retain messages for days and process them later, while we can take down our EC2 instances.

Q7. You are running a photo-sharing website where your images are downloaded from all over the world. Every month you publish a master pack of beautiful mountain images that are over 15 GB in size. The content is currently hosted on an Elastic File System (EFS) file system and distributed by an Application Load Balancer and a set of EC2 instances. Each month, you are experiencing very high traffic which increases the load on your EC2 instances and increases network costs. What do you recommend to reduce EC2 load and network costs without refactoring your website?

A. Create a CloudFront Distribution

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds. Amazon CloudFront can be used in front of an Application Load Balancer.

Q8. An AWS service allows you to capture gigabytes of data per second in real-time and deliver these data to multiple consuming applications, with a replay feature.

1. Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service. It can continuously capture gigabytes of data per second from hundreds of sources such as website clickstreams, database event streams, financial transactions, social media feeds, IT logs, and location-tracking events.

Databases on AWS Q&A Points –

Q1. Which database helps you store relational datasets, with SQL language compatibility and the capability of processing transactions such as insert, update, and delete?

1. Amazon RDS

Q2. Which AWS service provides you with caching capability that is compatible with Redis API?

1. Amazon ElastiCache is a fully managed in-memory data store, compatible with Redis or Memcached.

Q3. You want to migrate an on-premises MongoDB NoSQL database to AWS. You don't want to manage any database servers, so you want to use a managed NoSQL Serverless database, that provides you with high availability, durability, and reliability, and the capability to take your database global. Which database should you choose?

1. Amazon DynamoDB is a key-value, document, NoSQL database.

Q4. You are looking to perform Online Transaction Processing (OLTP). You would like to use a database that has built-in auto-scaling capabilities and provides you with the maximum number of replicas for its underlying storage. What AWS service do you recommend?

1. Amazon Aurora,

Amazon Aurora is a MySQL and PostgreSQL-compatible relational database. It features a distributed, fault-tolerant, self-healing storage system that auto-scales up to 128TB per database instance. It delivers high performance and availability with up to 15 low-latency read replicas, point-in-time recovery, continuous backup to Amazon S3, and replication across 3 AZs.

Q5. As a Solutions Architect, a startup company asked you for help as they are working on an architecture for a social media website where users can be friends with each other, and like each other's posts. The company plan on performing some complicated queries such as "What are the number of likes on the posts that have been posted by the friends of Mike?". Which database do you recommend?

1. Amazon Neptune,  
   Amazon Neptune is a fast, reliable, fully-managed graph database service that makes it easy to build and run applications that work with highly connected datasets.

Q6. You have a set of files, 100MB each, that you want to store in a reliable and durable key-value store. Which AWS service do you recommend?

1. Amazon S3 is indeed a key-value store! (where the key is the full path of the object in the bucket)

Q7. A company has an on-premises website that uses ReactJS as its frontend, NodeJS as its backend, and MongoDB for the database. There are some issues with the self-hosted MongoDB database as there is a lot of maintenance required and they don’t have and can’t afford the resources or experience to handle those issues. So, a decision was made to migrate the website to AWS. They have decided to host the frontend ReactJS application in an S3 bucket and the NodeJS backend on a set of EC2 instances. Which AWS service can they use to migrate the MongoDB database that provides them with high scalability and availability without making any code changes?

A. Amazon DocumentDB

Q8. A company using a self-hosted on-premises Apache Cassandra database which they want to migrate to AWS. Which AWS service can they use which provides them with a fully managed, highly available, and scalable Apache Cassandra database?

1. Amazon Keyspaces

Q9. An online payment company is using AWS to host its infrastructure. Due to the application’s nature, they have a strict requirement to store an accurate record of financial transactions such as credit and debit transactions. Those transactions must be stored in secured, immutable, encrypted storage which can be cryptographically verified. Which AWS service is best suited for this use case?

1. Amazon QLDB

Q10. A startup is working on developing a new project to reduce forest fires due to climate change. The startup is developing sensors that will be spread across the entire forest to make some readings such as temperature, humidity, and pressures which will help detect the forest fires before it happens. They are going to have thousands of sensors that are going to store a lot of readings each second. There is a requirement to store those readings and do fast analytics so they can predict if there is a fire. Which AWS service can they use to store those readings?

1. Amazon Timestream

Databases on AWS Q&A Points –

Q1. You would like to have a database that is efficient at performing analytical queries on large sets of columnar data. You would like to connect to this Data Warehouse using a reporting and dashboard tool such as Amazon QuickSight. Which AWS technology do you recommend?

1. Amazon Redshift

Q2. You have a lot of log files stored in an S3 bucket that you want to perform a quick analysis, if possible Serverless, to filter the logs and find users that attempted to make an unauthorized action. Which AWS service allows you to do so?

1. Amazon Athena

Q3. As a Solutions Architect, you have been instructed you to prepare a disaster recovery plan for a Redshift cluster. What should you do?

1. Enable automated snapshots, then configure your Redshift cluster to automatically copy snapshots to another AWS region

Q4. Which feature in Redshift forces all COPY and UNLOAD traffic moving between your cluster and data repositories through your VPCs?

1. Enhanced VPC Routing

Q5. You are running a gaming website that is using DynamoDB as its data store. Users have been asking for a search feature to find other gamers by name, with partial matches if possible. Which AWS technology do you recommend implementing this feature?

1. Amazon OpenSearch Service

Q6. An AWS service allows you to create, run, and monitor ETL (extract, transform, and load) jobs in a few clicks.

1. AWS Glue

Q7. A company is using AWS to host its public websites and internal applications. Those different websites and applications generate a lot of logs and traces. There is a requirement to centrally store those logs and efficiently search and analyze those logs in real-time for detection of any errors and if there is a threat. Which AWS service can help them efficiently store and analyze logs?

1. Amazon OpenSearch service

Q8. ……………………….. makes it easy and cost-effective for data engineers and analysts to run applications built using open-source big data frameworks such as Apache Spark, Hive, or Presto without having to operate or manage clusters.

1. Amazon EMR,

Amazon EMR is a cloud big data solution that lets you run and scale Apache Spark, Hive, and other open-source frameworks for data processing, analytics, and machine learning.

Q9. An e-commerce company has all its historical data such as orders, customers, revenues, and sales for the previous years hosted on a Redshift cluster. There is a requirement to generate some dashboards and reports indicating the revenues from the previous years and the total sales, so it will be easy to define the requirements for the next year. The DevOps team is assigned to find an AWS service that can help define those dashboards and have native integration with Redshift. Which AWS service is best suited?

1. Amazon QuickSight

Q10. Which AWS Glue feature allows you to save and track the data that has already been processed during a previous run of a Glue ETL job?

1. Glue Job Bookmarks

Q11. You are a DevOps engineer in a machine learning company which 3 TB of JSON files stored in an S3 bucket. There’s a requirement to do some analytics on those files using Amazon Athena and you have been tasked to find a way to convert those files’ format from JSON to Apache Parquet. Which AWS service is best suited?

1. AWS Glue, makes use of ETL feature to convert the JSON to Apache Parquet for data transformations.

Q12. You have an on-premises application that is used together with an on-premises Apache Kafka to receive a stream of clickstream events from multiple websites. You have been tasked to migrate this application as soon as possible without any code changes. You decided to host the application on an EC2 instance. What is the best option you recommend migrating Apache Kafka?

1. Amazon MSK, Managed Streaming for Kafka Services

Q13. You have data stored in RDS, S3 buckets and you are using AWS Lake Formation as a data lake to collect, move and catalog data so you can do some analytics. You have a lot of big data and ML engineers in the company, and you want to control access to part of the data as it might contain sensitive information. What can you use?

1. Lake Formation Fine-grained Access Control

AWS Lake Formation helps you centrally govern, secure, and globally share data for analytics and machine learning. With Lake Formation, you can manage fine-grained access control for your data lake data on Amazon Simple Storage Service (Amazon S3) and its metadata in AWS Glue Data Catalog.

Q14. Which AWS service is most appropriate when you want to perform real-time analytics on streams of data?

1. Amazon Kinesis Data Analytics - Use Kinesis Data Analytics with Kinesis Data Streams as the underlying source of data.

Machine Learning on AWS Q&A Points –

Q1. You should use Amazon Transcribe to turn text into lifelike speech using deep learning.

1. False,

Amazon Transcribe is an AWS service that makes it easy for customers to convert speech-to-text. Amazon Polly is a service that turns text into lifelike speech.

Q2. A company would like to implement a chatbot that will convert speech-to-text and recognize the customers' intentions. What service should it use?

1. Lex,

Amazon Lex is a service for building conversational interfaces into any application using voice and text. Lex provides the advanced deep learning functionalities of automatic speech recognition (ASR) for converting speech to text, and natural language understanding (NLU) to recognize the intent of the text, to enable you to build applications with highly engaging user experiences and lifelike conversational interactions.

Q3. Which fully managed service can deliver highly accurate forecasts?

1. Forecast,

Amazon Forecast is a fully managed service that uses machine learning to deliver highly accurate forecasts.

Q4. You would like to find objects, people, text, or scenes in images and videos. What AWS service should you use?

1. Rekognition,

Amazon Rekognition makes it easy to add image and video analysis to your applications using proven, highly scalable, deep learning technology that requires no machine learning expertise to use.

Q5. A start-up would like to rapidly create customized user experiences. Which AWS service can help?

1. Personalize,

Amazon Personalize is a machine learning service that makes it easy for developers to create individualized recommendations for customers using their applications.

Q6. A research team would like to group articles by topics using Natural Language Processing (NLP). Which service should they use?

1. Comprehend,

Amazon Comprehend is a natural language processing (NLP) service that uses machine learning to find meaning and insights in text.

Q7. A company would like to convert its documents into different languages, with natural and accurate wording. What should they use?

1. Translate,

Amazon Translate is a neural machine translation service that delivers fast, high-quality, and affordable language translation.

Q8. A developer would like to build, train, and deploy a machine learning model quickly. Which service can he use?

1. Sagemaker,

Amazon SageMaker is a fully managed service that provides every developer and data scientist with the ability to build, train, and deploy machine learning (ML) models quickly. SageMaker removes the heavy lifting from each step of the machine learning process to make it easier to develop high quality models.

Q9. Which AWS service makes it easy to convert speech-to-text?

1. Transcribe,

Amazon Transcribe is an AWS service that makes it easy for customers to convert speech-to-text.

Q10. Which of the following services is a document search service powered by machine learning?

1. Kendra,

Amazon Kendra is a highly accurate and easy to use enterprise search service that’s powered by machine learning.

Q11. A company is managing an image and video sharing platform which is used by customers around the globe. The platform is running on AWS using an S3 bucket to host both images and videos and using CloudFront as the CDN to deliver content to customers all over the world with low latency. In the last couple of months, a lot of customers have complained that they have started to see inappropriate content on the platform which started to increase in the last week. It will be very expensive and time-consuming to manually approve those images and videos by employees before its published on the platform. There is a requirement to find a solution that can automatically detect inappropriate and offensive images and videos and give you the ability to set a minimum confidence threshold for items that will be flagged and allows for manual review. Which AWS service can fit the requirement?

1. Amazon Rekognition

Q12. An online medical company that allows you to book an appointment with doctors using through a phone call is using AWS to host their infrastructure. They are using Amazon Connect and Amazon Lex to receive calls and create a workflow, book an appointment, and pay. According to the company’s policy, all calls must be recorded for review. But, there is a requirement to remove any Personally Identifiable Information (PII) from the call before it's saved. What do you recommend to use which helps in removing PII from calls?

1. Amazon Transcribe

Q13. Amazon Polly allows you to turn text into speech. It has two important features. First is ……………….. which allows you to customize the pronunciation of words (e.g., “Amazon EC2” will be “Amazon Elastic Compute Cloud”). The second is ……………….. which allows you to emphasize words, including breathing sounds, whispering, and more.

1. Pronunciation Lexicons, Speech Synthesis Markup Language (SSML)

Q14. A medical company is in the process of implementing a solution to detect, extract, and analyze information from unstructured medical text like doctors’ notes, clinical trial reports, and radiology reports. Those documents are uploaded and stored on S3 buckets. According to the company’s regulations, the solution must be designed and implemented to keep patients’ privacy by identifying Protected Health Information (PHI) so the solution will be eligible with HIPAA. Which AWS service should you use?

1. Amazon Comprehend Medical –

Monitoring and Auditing on AWS Q&A Points –

Q1. You have an RDS DB instance that's configured to push its database logs to CloudWatch. You want to create a CloudWatch alarm if there's an Error found in the logs. How would you do that?

1. Create a CloudWatch Logs Metric Filter that filters the logs for the keyword Error, then create a CloudWatch Alarm based on the Metric Filter.

Q2. You have an application hosted on a fleet of EC2 instances managed by an Auto Scaling Group that you configured its minimum capacity to 2. Also, you have created a CloudWatch Alarm that is configured to scale in your ASG when CPU Utilization is below 60%. Currently, your application runs on 2 EC2 instances and has low traffic, and the CloudWatch Alarm is in the ALARM state. What will happen?

1. The CloudWatch Alarm will remain in ALARM state but never decrease the number of EC2 instances in the ASG.

The number of EC2 instances in an ASG cannot go below the minimum capacity, even if the CloudWatch alarm would in theory trigger an EC2 instance termination.

Q3. How would you monitor your EC2 instance memory usage in CloudWatch?

A. Use the Unified CloudWatch Agent to push memory usage as a custom metric to CloudWatch

Q4. You have made a configuration change and would like to evaluate the impact of it on the performance of your application. Which AWS service should you use?

1. Amazon CloudWatch is a monitoring service that allows you to monitor your applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. It is used to monitor your applications' performance and metrics.

Q5. Someone has terminated an EC2 instance in your AWS account last week, which was hosting a critical database that contains sensitive data. Which AWS service helps you find who did that and when?

A. AWS CloudTrail,

AWS CloudTrail allows you to log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. It provides the event history of your AWS account activity, audit API calls made through the AWS Management Console, AWS SDKs, AWS CLI. So, the EC2 instance termination API call will appear here. You can use CloudTrail to detect unusual activity in your AWS accounts.

Q6. You have CloudTrail enabled for your AWS Account in all AWS Regions. What should you use to detect unusual activity in your AWS Account?

A. CloudTrail Insights

Q7. One of your teammates terminated an EC2 instance 4 months ago which has critical data. You don't know who made this, so you are going to review all API calls within this period using CloudTrail. You already have CloudTrail set up and configured to send logs to the S3 bucket. What should you do to find out who made this?

1. Analyze CloudTrail logs in S3 bucket using Amazon Athena

Q8. You are running a website on a fleet of EC2 instances with OS that has a known vulnerability on port 84. You want to continuously monitor your EC2 instances if they have port 84 exposed. How should you do this?

A. Setup Config Rules

Q9. You would like to evaluate the compliance of your resource's configurations over time. Which AWS service will you choose?

A. AWS Config

Q10. Someone changed the configuration of a resource and made it non-compliant. Which AWS service is responsible for logging who made modifications to resources?

A. AWS CloudTrail

Q11. You have enabled AWS Config to monitor Security Groups if there's unrestricted SSH access to any of your EC2 instances. Which AWS Config feature can you use to automatically re-configure your Security Groups to their correct state?

A. AWS Config Remediations

Q12. You are running a critical website on a set of EC2 instances with a tightened Security Group that has restricted SSH access. You have enabled AWS Config in your AWS Region and you want to be notified via email when someone modified your EC2 instances' Security Group. Which AWS Config feature helps you do this?

A. AWS Config Notifications

Q13. …………………………. is a CloudWatch feature that allows you to send CloudWatch metrics in near real-time to S3 bucket (through Kinesis Data Firehose) and 3rd party destinations (e.g., Splunk, Datadog, …).

A. CloudWatch Metric Stream

Q14. A DevOps engineer is working for a company and managing its infrastructure and resources on AWS. There was a sudden spike in traffic for the main application for the company which was not normal in this period of the year. The application is hosted on a couple of EC2 instances in private subnets and is fronted by an Application Load Balancer in a public subnet. To detect if this is normal traffic or an attack, the DevOps engineer enabled the VPC Flow Logs for the subnets and stored those logs in CloudWatch Log Group. The DevOps wants to analyze those logs and find out the top IP addresses making requests against the website to check if there is an attack. Which of the following can help the DevOps engineer to analyze those logs?

1. CloudWatch Contributor Insights

Q15. A company is developing a Serverless application on AWS using Lambda, DynamoDB, and Cognito. A junior developer joined a few weeks ago and accidentally deleted one of the DynamoDB tables in the dev AWS account which contained important data. The CTO asks you to prevent this from happening again and there must be a notification system to monitor if there is an attempt to make such deletion actions for the DynamoDB tables. What would you do?

1. Assign Developers to a certain IAM group which prevents deletion of DynamoDB tables. Configure EventBridge to capture any DeleteTable API calls through CloudTrail and send a notification using SNS.

Q16. A company has a running Serverless application on AWS which uses EventBridge as an inter-communication channel between different services within the application. There is a requirement to use the events in the prod environment in the dev environment to make some tests. The tests will be done every 6 months, so the events need to be stored and used later on. What is the most efficient and cost-effective way to store EventBridge events and use them later?

1. Using EventBridge Archive and Replay feature.

AWS IAM Advanced Questions Q&A Points –

Q1. You have strong regulatory requirements to only allow fully internally audited AWS services in production. You still want to allow your teams to experiment in a development environment while services are being audited. How can you best set this up?

1. Create an AWS Organization and create two Prod and Dev OUs, then Apply an SCP on the Prod OU

Q2. You are managing the AWS account for your company, and you want to give one of the developers access to read files from an S3 bucket. You have updated the bucket policy to this, but he still can't access the files in the bucket. What is the problem?

{

    "Version": "2012-10-17",

    "Statement": [{

        "Sid": "AllowsRead",

        "Effect": "Allow",

        "Principal": {

            "AWS": "arn:aws:iam::123456789012:user/Dave"

        },

        "Action": "s3:GetObject",

        "Resource": "arn:aws:s3:::static-files-bucket-xxx"

     }]

}

1. Change the resource to "arn:aws:s3:::static-files-bucket-xxx/\*", because this is an object-level permission.

Q3. You have 5 AWS Accounts that you manage using AWS Organizations. You want to restrict access to certain AWS services in each account. How should you do that?

1. Using AWS Organizations SCP

Q4. Which of the following IAM condition key you can use only to allow API calls to a specified AWS region?

1. “aws:RequestedRegion”

Q5. When configuring permissions for EventBridge to configure a Lambda function as a target you should use ………………….. but when you want to configure a Kinesis Data Streams as a target you should use …………………..

1. Resource-Based Policy, Identity-Based Policy

AWS Security and Encryption Quiz Q&A Points –

Q1. To enable In-flight Encryption (In-Transit Encryption), we need to have .......................

1. An HTTPS endpoint with an SSL certificate

In-flight Encryption = HTTPS, and HTTPS can not be enabled without an SSL certificate

Q2. Server-Side Encryption means that the data is sent encrypted to the server.

1. Server-Side Encryption means the server will encrypt the data for us. We don't need to encrypt it beforehand.

Q3. In Server-Side Encryption, where do the encryption and decryption happen?

1. Both Encryption and Decryption happens on the server side, in Server-Side Encryption, we can't do encryption/decryption ourselves as we don't have access to the corresponding encryption key.

Q4. In Client-Side Encryption, the server must know our encryption scheme before we can upload the data.

1. False,

With Client-Side Encryption, the server doesn't need to know any information about the encryption scheme being used, as the server will not perform any encryption or decryption operations.

Q5. You need to create KMS Keys in AWS KMS before you are able to use the encryption features for EBS, S3, RDS ...

1. False,

You can use the AWS Managed Service keys in KMS, therefore we don't need to create our own KMS keys.

Q6. AWS KMS supports both symmetric and asymmetric KMS keys.

1. True,

KMS keys can be symmetric or asymmetric. A symmetric KMS key represents a 256-bit key used for encryption and decryption. An asymmetric KMS key represents an RSA key pair used for encryption and decryption or signing and verification, but not both. Or it represents an elliptic curve (ECC) key pair used for signing and verification.

Q7. When you enable Automatic Rotation on your KMS Key, the backing key is rotated every .................

1. 1 Year

Q8. You have an AMI that has an encrypted EBS snapshot using KMS CMK. You want to share this AMI with another AWS account. You have shared the AMI with the desired AWS account, but the other AWS account still can't use it. How would you solve this problem?

1. You need to share the KMS CMK used to encrypt the AMI with the other AWS account.

Q9. You have created a Customer-managed CMK in KMS that you use to encrypt both S3 buckets and EBS snapshots. Your company policy mandates that your encryption keys be rotated every 3 months. What should you do?

1. Rotate the KMS CMK manually, create a new KMS CMK and use Key aliases to reference the new KMS CMK. Keep the old KMS CMK so you can decrypt the old data.

Q10. What should you use to control access to your KMS CMKs?

1. KMS Key Policies

Q11. You have a Lambda function used to process some data in the database. You would like to give your Lambda function access to the database password. Which of the following options is the most secure?

1. Have it as an encrypted environment variable and decrypt it at runtime.

Q12. You have a secret value that you use for encryption purposes, and you want to store and track the values of this secret over time. Which AWS service should you use?

1. SSM Parameter Store,

SSM Parameters Store can be used to store secrets and has built-in version tracking capability. Each time you edit the value of a parameter, SSM Parameter Store creates a new version of the parameter and retains the previous versions. You can view the details, including the values, of all versions in a parameter's history.

Q13. Your user-facing website is a high-risk target for DDoS attacks and you would like to get 24/7 support in case they happen and AWS bill reimbursement for the incurred costs during the attack. What AWS service should you use?

1. AWS Shield Advanced

Q14. You would like to externally maintain the configuration values of your main database, to be picked up at runtime by your application. What's the best place to store them to maintain control and version history?

1. SSM Parameter Store

Q15. AWS GuardDuty scans the following data sources, EXCEPT ...............

1. CloudWatch Logs

Q16. You have a website hosted on a fleet of EC2 instances fronted by an Application Load Balancer. What should you use to protect your website from common web application attacks (e.g., SQL Injection)?

1. AWS WAF

Q17. You would like to analyze OS vulnerabilities from within EC2 instances. You need these analyses to occur weekly and provide you with concrete recommendations in case vulnerabilities are found. Which AWS service should you use?

1. Amazon Inspector

Q18. What is the most suitable AWS service for storing RDS DB passwords which also provides you automatic rotation?

1. AWS Secrets Manager

Q19. Which AWS service allows you to centrally manage EC2 Security Groups and AWS Shield Advanced across all AWS accounts in your AWS Organization?

1. AWS Firewall Manager,

AWS Firewall Manager is a security management service that allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organizations. It is integrated with AWS Organizations so you can enable AWS WAF rules, AWS Shield Advanced protection, security groups, AWS Network Firewall rules, and Amazon Route 53 Resolver DNS Firewall rules.

Q20. Which AWS service helps you protect your sensitive data stored in S3 buckets?

1. AWS Macie,

Amazon Macie is a fully managed data security service that uses Machine Learning to discover and protect your sensitive data stored in S3 buckets. It automatically provides an inventory of S3 buckets including a list of unencrypted buckets, publicly accessible buckets, and buckets shared with other AWS accounts. It allows you to identify and alert you to sensitive data, such as Personally Identifiable Information (PII).

Q21. An online-payment company is using AWS to host its infrastructure. The frontend is created using VueJS and is hosted on an S3 bucket and the backend is developed using PHP and is hosted on EC2 instances in an Auto Scaling Group. As their customers are worldwide, they use both CloudFront and Aurora Global database to implement multi-region deployments to provide the lowest latency and provide availability, and resiliency. A new feature required which gives customers the ability to store data encrypted on the database and this data must not be disclosed even by the company admins. The data should be encrypted on the client side and stored in an encrypted format. What do you recommend to implement this?

1. Use Aurora Client-side Encryption and KMS Multi-region Keys

Q22. You have an S3 bucket that is encrypted with SSE-KMS. You have been tasked to replicate the objects to a target bucket in the same AWS region but with a different KMS Key. You have configured the S3 replication, the target bucket, and the target KMS key and it is still not working. What is missing to make the S3 replication work?

1. Configure permissions for both Source KMS Key kms:Decrypt and Target KMS Key kms:Encrypt

to be used by the S3 Replication Service.

Q23. You have generated a public certificate using LetsEncrypt and uploaded it to the ACM so you can use and attach to an Application Load Balancer that forwards traffic to EC2 instances. As this certificate is generated outside of AWS, it does not support the automatic renewal feature. How would you be notified 30 days before this certificate expires so you can manually generate a new one?

1. Configure EventBridge for Daily Expiration Events from ACM to invoke SNS notifications to your email.

Q24. You have created the main Edge-Optimized API Gateway in us-west-2 AWS region. This main Edge-Optimized API Gateway forwards traffic to the second level API Gateway in ap-southeast-1. You want to secure the main API Gateway by attaching an ACM certificate to it. Which AWS region are you going to create the ACM certificate in?

1. Other than us-west-2 and ap-southeast-1, As the Edge-Optimized API Gateway is using a custom AWS managed CloudFront distribution behind the scene to route requests across the globe through CloudFront Edge locations, the ACM certificate must be created in us-east-1.

Q25. You are managing an AWS Organization with multiple AWS accounts. Each account has a separate application with different resources. You want an easy way to manage Security Groups and WAF Rules across those accounts as there was a security incident the last week and you want to tighten up your resources. Which AWS service can help you to do so?

1. AWS Firewall Manager

AWS Network - VPC Quiz Q&A Points –

Q1. What does this CIDR 10.0.4.0/28 correspond to?

1. 10.0.4.0 to 10.0.4.15

/28 means 16 IPs (=2^(32-28) = 2^4), means only the last digit can change.

Q2. You have a corporate network of size 10.0.0.0/8 and a satellite office of size 192.168.0.0/16. Which CIDR is acceptable for your AWS VPC if you plan on connecting your networks later?

1. 172.16.0.0/16

CIDR not should overlap, and the max CIDR size in AWS is /16.

Q3. You plan on creating a subnet and want it to have at least capacity for 28 EC2 instances. What's the minimum size you need to have for your subnet?

1. 64 Ips - /26

Q4. Security Groups operate at the ................. level while NACLs operate at the ................. level.

1. EC2, Instance, Subnet

Q5. You have attached an Internet Gateway to your VPC, but your EC2 instances still don't have access to the internet. What is NOT a possible issue?

1. The Security Group does not allow traffic in. Security groups are stateful and if traffic can go out, then it can go back in.

Q6. You would like to provide Internet access to your EC2 instances in private subnets with IPv4 while making sure this solution requires the least amount of administration and scales seamlessly. What should you use?

1. NAT Gateway

Q7. VPC Peering has been enabled between VPC A and VPC B, and the route tables have been updated for VPC A. But the EC2 instances cannot communicate. What is the likely issue?

1. Check the Route Tables in VPC B

Route Tables must be updated in both VPCs that are peered.

Q8. You have set up a Direct Connect connection between your corporate data center and your VPC A in your AWS account. You need to access VPC B in another AWS region from your corporate datacenter as well. What should you do?

1. Use a Direct Connect Gateway

This is the main use case of Direct Connect Gateways.

Q9. When using VPC Endpoints, what are the only two AWS services that have a Gateway Endpoint available?

1. Amazon S3 & DynamoDB

These two services have a VPC Gateway Endpoint (remember it), all the other ones have an Interface endpoint (powered by Private Link - means a private IP).

Q10. AWS reserves 5 IP addresses each time you create a new subnet in a VPC. When you create a subnet with CIDR 10.0.0.0/24, the following IP addresses are reserved, EXCEPT ....................

1. 10.0.0.4

Q11. You have 3 VPCs A, B, and C. You want to establish a VPC Peering connection between all the 3 VPCs. What should you do?

1. Establish a 3 VPC. Peering connections (A-B,A-C,B-C)

Q12. How can you capture information about IP traffic inside your VPCs?

1. Enable VPC Flow Logs

Q13. If you want a 500 Mbps Direct Connect connection between your corporate datacenter to AWS, you would choose a .................. connection.

1. Hosted,

Hosted

19. When you set up an AWS Site-to-Site VPN connection between your corporate on-premises datacenter and VPCs in AWS Cloud, what are the two major components you want to configure for this connection?

A. Virtual Private Gateway and Customer Gateway

Q15. Your company has several on-premises sites across the USA. These sites are currently linked using private connections, but your private connections provider has been recently quite unstable, making your IT architecture partially offline. You would like to create a backup connection that will use the public Internet to link your on-premises sites, that you can failover in case of issues with your provider. What do you recommend?

1. AWS VPN CloudHub

AWS VPN CloudHub allows you to securely communicate with multiple sites using AWS VPN. It operates on a simple hub-and-spoke model that you can use with or without a VPC.

Q16. You need to set up a dedicated connection between your on-premises corporate datacenter and AWS Cloud. This connection must be private, consistent, and traffic must not travel through the Internet. Which AWS service should you use?

1. AWS Direct Connect

Q17. Using a Direct Connect connection, you can access both public and private AWS resources.

1. True

Establishes a direct connection between on-premises and AWS VPC

Q18. You want to scale up an AWS Site-to-Site VPN connection throughput, established between your on-premises data and AWS Cloud, beyond a single IPsec tunnel's maximum limit of 1.25 Gbps. What should you do?

1. Use Transit Gateway

Q19. You have a VPC in your AWS account that runs in a dual-stack mode. You are continuously trying to launch an EC2 instance, but it fails. After further investigation, you have found that you are no longer have IPv4 addresses available. What should you do?

1. Add an additional IPv4 CIDR to your VPC

Q20. A web application backend is hosted on EC2 instances in private subnets fronted by an Application Load Balancer in public subnets. There is a requirement to give some of the developers access to the backend EC2 instances but without exposing the backend EC2 instances to the Internet. You have created a bastion host EC2 instance in the public subnet and configured the backend EC2 instances Security Group to allow traffic from the bastion host. Which of the following is the best configuration for bastion host Security Group to make it secure?

1. Allow traffic only on port 22 from the company’s public CIDR

Q21. A company has set up a Direct Connect connection between their corporate data center to AWS. There is a requirement to prepare a cost-effective secure backup connection in case there are issues with this Direct Connect connection. What is the most cost effective and secure solution you recommend?

1. Setup a Site-to-Site VPN connection as a backup.

Q22. Which AWS service allows you to protect and control traffic in your VPC from layer 3 to layer 7?

1. AWS Network Firewall

Q23. A web application hosted on a fleet of EC2 instances managed by an Auto Scaling Group. You are exposing this application through an Application Load Balancer. Both the EC2 instances and the ALB are deployed on a VPC with the following CIDR 192.168.0.0/18. How do you configure the EC2 instances' security group to ensure only the ALB can access them on port 80?

1. Add an Inbound Rule with port 80 and ALB’s Security Group as the source.

This is the most secure way of ensuring only the ALB can access the EC2 instances. Referencing by security groups in rules is an extremely powerful rule and many questions at the exam rely on it. Make sure you fully master the concepts behind it!

Disaster Recovery & Migration Quiz Q&A Points –

Q1. As part of your Disaster Recovery plan, you would like to have only the critical infrastructure up and running in AWS. You don't mind a longer Recovery Time Objective (RTO). Which DR strategy do you recommend?

1. Pilot Light


      Graph showing disaster recovery strategies and highlights of each strategy.
    

<- High RPO and RTO Lower RPO and RTO->

Q2. You would like to get the Disaster Recovery strategy with the lowest Recovery Time Objective (RTO) and Recovery Point Objective (RPO), regardless of the cost. Which DR should you choose?

1. Multi-Site

Q3. Which of the following Disaster Recovery strategies has a potentially high Recovery Point Objective (RPO) and Recovery Time Objective (RTO)?

1. Backup and Restore

Q4. You want to make a Disaster Recovery plan where you have a scaled-down version of your system up and running, and when a disaster happens, it scales up quickly. Which DR strategy should you choose?

1. Warm Standby

Q5. You have an on-premises Oracle database that you want to migrate to AWS, specifically to Amazon Aurora. How would you do the migration?

1. Use AWS Schema Conversion Tool (AWS SCT) to convert the database schema, then use AWS Database Migration Service (AWS DMS) to migrate the data.

Q6. AWS DataSync supports the following locations, EXCEPT ....................

1. Amazon EBS

Q7. You are running many resources in AWS such as EC2 instances, EBS volumes, DynamoDB tables... You want an easy way to manage backups across all these AWS services from a single place. Which AWS offering makes this process easy?

1. AWS Backup

AWS Backup enables you to centralize and automate data protection across AWS services. It helps you support your regulatory compliance or business policies for data protection.

Q8. A company planning to migrate its existing websites, applications, servers, virtual machines, and data to AWS. They want to do a lift-and-shift migration with minimum downtime and reduced costs. Which AWS service can help in this scenario?

1. AWS Application Migration Service

Q9. A company is using VMware on its on-premises data center to manage its infrastructure. There is a requirement to extend their data center and infrastructure to AWS but keep using the technology stack they are using which is VMware. Which AWS service can they use?

1. VMware Cloud on AWS

Q10. A company is using RDS for MySQL as their main database but, lately they have been facing issues in managing the database, performance issues, and the scalability. And they have decided to use Aurora for MySQL instead for better performance, less complexity and less administrative tasks required. What is the best way and most cost-effective way to migrate from RDS for MySQL to Aurora for MySQL?

1. Create a snapshot from RDS for MySQL and restore it to Aurora for MySQL

Q11. Which AWS service can you use to automate the backup across different AWS services such as RDS, DynamoDB, Aurora, and EFS file systems, and EBS volumes?

1. AWS Backup