First test Score 61%

1. Compute - EC2, Lambda, EBS, Load Balancing, Beanstalk
2. Storage - S3, Redshift, Storage Gateway, EFS, Glacier
3. Networking - VPC, Route53, API Gateway, CLoudFront
4. Security - IAM, KMS, Cognito
5. Governance - OpsWork, Cost Explorer, CloudTrail, CloudWatch
6. Databases - DynamoDB, RDS, Elasticache
7. Applications - SNS, SQS, SWF,

It is always a good idea to do some practice questions, I did some 400 of them and scored 87%.

Instead of buying them on some obscure site, I got an eBook named “AWS Certified Solutions Architect Associate (SAA-C01) - Practice Questions 2019 (800+): by Rehan Haider. Simply search for the ASIN on Amazon “**B07YG6NNW3**”

---------------

When to do read replica vs snapshot of RDS?

Aws shield – for ddos attacks

Scenarios with elb and auto scaling – how are instances terminated. Default vs. specific configuration

1. C - Deploy database instances in private subnet
2. I - Redis is being used for Elasticache, and you need to protect the access to ElastiCache cluster where redis commands can be entered
   1. Create new Redis Cluster with –transit-encryption-enabled and –auth-token params enabled
3. I – You’re using S3, and now have a new membership category. There is a requirement to provide access to multiple private media files to paying subs **without having to change current URLs**.
   1. The key is without having to change current URLs so you **don’t** use signed URLs which rotate. *Correct* answer is Use Signed Cookies, by sending required Set-Cookie to paying subscribers.

CloudFront signed URLs and signed cookies provide the same basic functionality: they allow you to control who can access your content. If you want to serve private content through CloudFront and you're trying to decide whether to use signed URLs or signed cookies, consider the following:

Use **signed URLs** for the following cases:

- You want to use an RTMP distribution. Signed cookies aren't supported for RTMP distributions.

- You want to restrict access to individual files, for example, an installation download for your application.

- Your users are using a client (for example, a custom HTTP client) that doesn't support cookies.

Use **signed cookies** for the following cases:

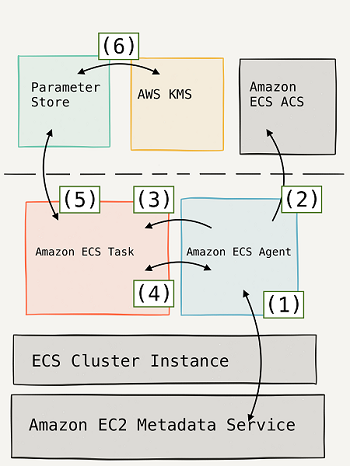
- You want to provide access to multiple restricted files, for example, all of the files for a video in HLS format or all of the files in the subscribers' area of a website.

- You don't want to change your current URLs.

1. C - A startup wants to cache data in memory – Elasticache
2. I – want to migrate on-prem IPs into AWS – Create Route Origin Authorization (ROA), then provision and advertise imported IPs to aws account.
3. C - On-Demand EC2 instance that is transferring large amounts of data to an Amazon S3 bucket in the same region – no cost
4. C - During the audit activities, it was noted that you are using a combination of Standard and Scheduled Reserved EC2 instances in your applications. Why vs. spot instances? – You can have capacity reservations on daily, weekly, monthly basis AND reserved instances don’t get interrupted
5. C – travel photo sharing on s3 is being linked to by other websites. How to mitigate? – use pre-signed URLs with expiry dates.
6. C – You use S3 One Zone IA for free users and S3 Standard IA for paying users. Why, whats the difference?
   1. S3 One Zone IA costs less than S3 Standard-IA
   2. S3-IA stores data in single AZ
7. C - Scale in policy of Auto Scaling is triggered, which instance will go first?
   1. EC2 launched from oldest launch config

Scale in works based on keeping all AZs available, and then terminating instance with oldest launch config

1. I - A RDS instance running in one AZ. High availability?
   1. RDS DB instance as multi-AZ deployment (NOT Read replica – performance only)
2. I - An online medical system hosted in AWS stores sensitive Personally Identifiable Information (PII) of the users in an Amazon S3 bucket. **Both the master keys** and **the unencrypted data** should never be sent to AWS to comply with the strict compliance and regulatory requirements of the company.
   1. Use S3 client side encryption with client-side master key
3. C – Use Macie to monitor and detect usage patterns in S3 data
4. I - To ensure that your RDS database can only be accessed using the profile credentials specific to your EC2 instances via an authentication token.
   1. Enable IAM DB Auth (for mysql and PostgreSQL) – this is required for the DB to accept auth via IAM, hence attaching a role to EC2 is not sufficient
5. C – an application is used extensively during working hours.
   1. Turn on schedule based scaling
6. I -- There are a lot of outages in the Availability Zone of your RDS database instance to the point that you have lost access to the database. What could you do to prevent losing access to your database in case that this event happens again?
   1. Enable multi-AZ failover
7. C – ssh from specific ip
   1. Enable inbound rule in SG from that ip with a /32 cidr
8. I - The application has a message broker service which uses industry standard messaging APIs and protocols that must be migrated as well, without rewriting the messaging code in your application.
   1. Amazon MQ
      1. **Amazon SQS** is incorrect because although this is a fully managed message queuing service, it does not support an extensive list of industry-standard messaging APIs and protocol, unlike Amazon MQ.
9. C - Data lost in instance store after shutting off. Cause?
   1. Instance stores are cleared after restart
10. C – Prevent DDoS attacks in AWS?
    1. Use AWS Shield which specifically helps with DDoS
11. I - What combination of the following options will protect the S3 objects in your bucket from both accidental deletion and overwriting? (Select TWO.)
    1. Enable Versioning
    2. Enable MFA delete (We don’t need to disallow S3 deletes using IAM bucket policy, just protect against them. This will prevent deletes altogether)
12. I - One of the engineers accidentally deleted a file hosted in Amazon S3 which has caused disruption of service. What can you do to prevent this from happening again?
    1. MFA and Versioning (Same as last question)
13. C – Ephemeral storage question. What happens when instance is stopped?
    1. Data is deleted
14. For an ECS container using Fargate as lunch type, credentials must be applied as env vars. Most not be saved as plain text. How to best implement?
    1. Use AWS Systems Mgr **Parameter Store** to keep the credentials. Encrypt via AWS KMS. Create IAM role for ECS task execution role (taskRoleArn) and reference it with your task definition which allows access to both KMS and Param Store. In container definition, specify secrets with the name of env variable to set in container which pulls from full ARN of Sys Mgr Param Store param with the creds



1. C- You must improve a DynamoDB table performance by distributing the workload evenly and using provisioned throughput efficiently
   1. Use partition keys with high cardinality which have large number of distinct values of each item (keyword: Evenly) [Essentially have a lot of buckets that the data can go into]
2. C - The security policy requires that the application hosted in EC2 encrypts the data first before writing it to the disk for storage.
   1. Use AWS KMS API to encrypt prior to writing data to disk
3. C – For an application, an ELB is used to distribute incoming requests across an auto-scaled group of EC2 instances. Autoscaling configuration is default. What happens when an EC2 instance behind an ELB fails a health check?
   1. ELB stops sending traffic to that instance
      1. This is because the auto-scaling group is configured with default settings where it only monitors “EC2 health” check types *and not ELB*
4. I - A telecommunications company is planning to give AWS Console access to developers. Company policy mandates the use of identity federation and role-based access control. Currently, the roles are already assigned using groups in the corporate Active Directory. What 2 options allow this access?
   1. AWS Directory Service AD Connector
   2. IAM Roles– You can assign an IAM Role to users or groups from your AD Directory (Apply IAM Roles to AD groups. IAM groups are IAM user collections)
5. I – You have a startup in early phases. How to manage the budgets for all AWS resources?
   1. AWS Budgets. (Selected Cost Explorer which is incorrect because explorer is just a visualizer)
6. C - You have load balancer doing health checks on ec2 instances. What happens when one ec2 fails a health check?
   1. Application Load Balancer stops sending traffic to the instance
7. I - Crypto traffic surge, how can you *protect* backend system from traffic spikes?
   1. Throttling limits in API GW
8. I - You are designing a multi-tier web application architecture that consists of a fleet of EC2 instances and an Oracle relational database server. It is required that the database is highly available and that you have full control over its underlying operating system. Which AWS service will you use for your database tier?
   1. EC2 instances with data replication between two AZs
      1. Not RDS with Multi-AZ deployments because RDS is an AWS managed service that doesn’t give you access to internals
9. I - A traffic monitoring and reporting application uses Kinesis to accept real-time data. In order to process and store the data, they used Amazon Kinesis Data Firehose to load the streaming data to various AWS resources. Which of the following services can you load streaming data into?
   1. Elasticache Service (Other options are subsets of S3 and Redshift – Firehose **can** load data into S3 and Redshift services indeed)
10. C - A company wants to store their data in AWS and retrieve it via SMB (could also be NFS potentially)
    1. Use AWS Storage gateway to launch a new file gateway that connects on-prem data center to AWS
11. C – High throughput and random IO operations to a DB
    1. Use Provisioned IOPS SSD
12. C - Need a HPC file system for hot storage and a cost effective cold storage
    1. Amazon FSx for Lustre for hot and S3 for cold storage
13. C - A popular social network is hosted in AWS and is using a DynamoDB table as its database. There is a requirement to implement a 'follow' feature where users can subscribe to certain updates made by a particular user and be notified via email. Which of the following is the most suitable solution that you should implement to meet the requirement?
    1. Enable DynamoDB Streams, Create AWS Lambda trigger from a DynamoDB Stream, an IAM role and publish message to SNS topic for notifying subscribers
    2. (Optionally using Kinesis Client Library for this also works, but that option did not enable Dynamo DB Streams as a step)
14. I - You want to monitor your EC2 instances based on a particular metric, which is not readily available in CloudWatch. Which of the following is a custom metric in CloudWatch which you have to manually set up?
    1. Memory Utilization

Available – cpu, network i/o, disk read/write. **Not** available: memory utilization, disk space utilization, and many others which can be collected by setting up a custom metric.

1. C - scalable, high throughput POSIX-compliant file system?
   1. EFS
2. C - Your manager instructed you to avoid using fully-managed AWS services and instead, only use specific services which allows you to access the underlying operating system for the resource.
   1. EC2
   2. EMR
3. I - Tightly managing the data flow of your Amazon Redshift cluster. One of the requirements is to use VPC flow logs to monitor all the COPY and UNLOAD traffic of your Redshift cluster that moves in and out of your VPC. Which of the following is the most suitable solution to implement in this scenario?
   1. Enable enhanced VPC routing on your Redshift cluster

When you use Amazon Redshift Enhanced VPC Routing, Amazon Redshift forces all COPY and UNLOAD traffic between your cluster and your data repositories through your Amazon VPC. You cannot enable flow logs without first enabling this.

If Enhanced VPC Routing is not enabled, Amazon Redshift routes traffic through the Internet, including traffic to other services within the AWS network.

1. C - database that can scale globally and can handle frequent schema changes.
   1. DynamoDB
2. I – A financial platform is hosted in your on-premises data center and uses an Oracle database. Due to a recent cooling problem in their data center, the company urgently needs to migrate their infrastructure to AWS to improve the performance of their applications. You are responsible in ensuring that the database is properly migrated and should remain available in case of database server failure in the future. Which of the following is the most suitable solution to meet the requirement?
   1. Create Oracle db in RDS with multi-AZ deployments.
3. C – Access AWS resources using on-prem credentials
   1. Use SMAL 2.0 based federation by using Microsoft AD FS
4. C – Monitor API Calls for Redshift Cluster instance
   1. CloudTrail for security logs
5. I - An application is hosted in an AWS Fargate cluster that runs a batch job whenever an object is loaded on an Amazon S3 bucket. The minimum number of ECS Tasks is initially set to 1 to save on costs, and it will only increase the task count based on the new objects uploaded on the S3 bucket. Once processing is done, the bucket becomes empty and the ECS Task count should be back to 1. Which is the most suitable option to implement with the LEAST amount of effort?
6. C - A new relational database is needed that autoscales capacity to meet the needs of the application's peak load and scales back down when the surge of activity is over.
   1. Aurora Serverlss with min and max cluster capacity
7. I - You’re setting up 1200 employees with access to their docs in S3. Which of the following will you need to consider so you can set up a solution that incorporates single sign-on feature from your corporate AD or LDAP directory and also restricts access for each individual user to a designated user folder in an S3 bucket?
   1. Configure IAM Role and IAM Policy to access the bucket
   2. Set up Federation proxy or Id provider and use AWS Security Token Service to gen temporary tokens

* Remember to read question carefully!! Multiple answers usually map to multiple requirements in the question

1. C - Considering that the Lambda function is storing sensitive database and API credentials, how can you secure this information to prevent other developers in your team, or anyone, from seeing these credentials in plain text?
   1. Create new KMS key and use it to enable encryption helpers that leverage AWS KMS to encrypt sensitive info
2. I - A popular social media website uses a CloudFront web distribution to serve their static contents to their millions of users around the globe. They are receiving a number of complaints recently that their users take a lot of time to log into their website. There are also occasions when their users are getting HTTP 504 errors. You are instructed by your manager to significantly reduce the user's login time to further optimize the system.

Which of the following options should you use together to set up a **cost-effective** solution that can improve your application's performance?

* 1. Set up origin failover by creating origin group with two origins
  2. Customize content that CF web distribution delivers using Lambda@Edge which allow auth via lambda at location closest to users.

1. C - App in EC2 consuming SQS msgs. The messages are getting processed multiple times
   1. App is not deleting messages in SQS after processing them.
2. I – How to prepare for disaster recovery with On-Demand EC2 instances behind Auto-Scaling with AMI from one region to another?
   1. Copy AMI and create new Auto Scaling group in us-west-2 to use the AMI ID (This is a better answer because just copying over the AMI remains some steps to be taken)
3. C – How to blacklist suspicious traffic coming in from certain IPs?
   1. Modfy NACLs associated with public subnets in VPC to deny access
4. C - Need to direct the write operations of production traffic to high capacity instances and reporting queries to internal staff to low capacity instances
   1. Create a custom endpoint in Aurora based on production traffic needs and another custom endpoint to handle reporting queries
5. C - IAM Bucket policy question
   1. Make sure to read multiple Effect, Action, Resource values
6. I – CIO wants to streamline organization through AWS to manage accounts, and share resources centrally
   1. Consolidate company accounts using AWS Organizations
   2. Use AWS Resource Access Mgr to easily and securely share your resources with your AWS accounts.

Got this one wrong for not reading the 2 requiements and mapping them to answers

1. C - A mobile game uses CF, Lambda, DynamoDB. Player data is in DynamoDB and static assets distributed by CF. Many complaints that saving and retrieving player info is taking long time. Which service will reduce DynamoDB response time from ms to microseconds?
   1. DAX
2. C - How can S3 encrypt your data?
   1. S3 Server Side
   2. S3 Client Side
3. C- You must monitor memory and disk utilization of your instances. How?
   1. Install CW agent to EC2 which gathers memory and disk utilization data. View custom metrics in Amazon CW console.
4. I - The application is heavily using the RDS instance to process complex read and write database operations. To maintain the reliability, availability, and performance of your systems, you must closely monitor how the different processes or threads on a DB instance use the CPU, including the percentage of the CPU bandwidth and total memory consumed by each process.
   1. Enable enhanced monitoring in RDS
5. C – How to set up tracking of various changes in AWS resources:
   1. Set up **cloud Trail** in s3 bucket using AWS cli, encrypt files with KMS and apply MFA delete on these logs
6. C - Add Js on webpages to make authenticated HTTP GET requests, Web browser is blocking javascript from allowing those requests
   1. Enable CORS in the S3 bucket
7. C - Help an organization build scalable using stateless web servers. Which AWS services to use for storing session data?
   1. DynamoDB
   2. Elasticache
8. C - How to make NAT Gateway deployment resilient?
   1. Create a NAT GW in each AZ. Configure route table in each private subnet to the NAT GW in that AZ
9. I - You are using a combination of API Gateway and Lambda for the web services of your online web portal that is being accessed by hundreds of thousands of clients each day. Your company will be announcing a new revolutionary product and it is expected that your web portal will receive a massive number of visitors all around the globe. How can you **protect** your backend systems and applications from traffic spikes?
   1. Throttle API Gateway

Test 2

<https://tutorialsdojo.com/latency-routing-vs-geoproximity-routing-vs-geolocation-routing/>

SES – simple email Service

STS – simple token service

AWS OpsWorks – chef and puppet