Question : 1 of 15 - Multiple Choice — Graded

Which is an operational process performed by AWS for data security?

Incorrect — Time spent : 7 sec

Your answer

A. AES-256 encryption of data stored on any shared storage device
B. Decommissioning of storage devices using industry-standard practices
C. Background virus scans of EBS volumes and EBS snapshots
D. Replication of data across multiple AWS Regions
E. Secure wiping of EBS data when an EBS volume is un-mounted

Correct Answer

B. Decommissioning of storage devices using industry-standard practices

Explanation

Correct answer is **B**

Storage Decommissioning

- *When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals.*
- *AWS uses the techniques detailed in DoD 5220.22-M (National Industrial Security Program Operating Manual) or NIST 800-88 (Guidelines for Media Sanitization) to destroy data as part of the decommissioning process.*
- *All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.*

Refer AWS Security Whitepaper

Option A is wrong as it is User responsibility

Option B is wrong as No virus scan is performed by AWS on User instances

Option C is wrong as AWS does not replicate data across regions unless done by User

Option D is wrong as data is not wiped off on EBS volume when unmounted and it can be remounted on other EC2 instance

AWS SAA-C01 Question feedback

Question : 2 of 15 - Multiple Choice — Graded

A customer has a web application that uses cookie-based sessions to track logged-in users. It is deployed on AWS using Elastic Load Balancing and Auto Scaling. When load increases, Auto Scaling launches new instances, but the load on the other instances does not decrease; this causes all existing users to have a slow experience. What could be the cause of the poor user experience?

Incorrect — Time spent : 18 sec

Your answer

A. ELB DNS record's TTL is set too high.
B. The new instances are not being added to the ELB during the Auto Scaling cooldown period.
C. The website uses the dynamic content feature of Amazon CloudFront which is keeping connections alive to the ELB.
D. ELB is continuing to send requests with previously established sessions to the same backend instances rather than spreading them out to the new instances.

Correct Answer

D. ELB is continuing to send requests with previously established sessions to the same backend instances rather than spreading them out to the new instances.

Explanation

Correct answer is **D** as ELB is stateful and uses cookie-based sessions. So it might be continuing to send requests to previously established sessions and hence existing users having a poor experience.

Option A is wrong as Elastic Load Balancing uses a TTL setting on the DNS record of 60 seconds and there is no mention of what is the configuration.

Option B is wrong as instances would still be added to reduce a load and only new instances after those would depend on the cooldown period.

Option C is wrong as CloudFront will route traffic back to the origin servers depending on the TTL.

AWS SAA-C01 Question feedback

Question : 3 of 15 - Multiple Choice — Graded

A user has created a photo editing software and hosted it on EC2. The software accepts requests from the user about the photo format and resolution and sends a message to S3 to enhance the picture accordingly. Which of the below mentioned AWS services will help make a scalable software with the AWS infrastructure in this scenario?

Incorrect — Time spent : 12 sec

Your answer

A. AWS Glacier
B. AWS Elastic Transcoder
C. AWS Simple Notification Service
D. AWS Simple Queue Service

Correct Answer

D. AWS Simple Queue Service

Explanation

Correct answer is **D** as SQS can be used to build scalable & decoupled software. SQS can be used to store messages, with files in S3 and process and scale accordingly.

Option A is wrong as Glacier is an archival storage solution.

Option B is wrong as Elastic Transcoder is a managed service for transcoding videos in different format.s

Option C is wrong as SNS is publish/subscribe messaging service.

AWS SAA-C01 Question feedback

Question : 4 of 15 - Multiple Choice — Graded

An application running on EC2 instances processes sensitive information stored on Amazon S3. The information is accessed over the Internet. The security team is concerned that the Internet connectivity to Amazon S3 is a security risk. Which solution will resolve the security concern?

Incorrect — Time spent : 5 sec

Your answer

A. Access the data through an Internet Gateway.
B. Access the data through a VPN connection.
C. Access the data through a NAT Gateway.
D. Access the data through a VPC endpoint for Amazon S3.

Correct Answer

D. Access the data through a VPC endpoint for Amazon S3.

Explanation

Correct answer is **D** as VPC endpoints allows EC2 instances to access S3 without traversing through internet.

Refer AWS documentation - VPC Endpoints

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

Endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in your VPC and services without imposing availability risks or bandwidth constraints on your network traffic.

Option A and C are wrong as NAT Gateways and Internet Gateways route traffic over the Internet to the public endpoint for Amazon S3.

Option B is wrong as there is no way to connect to Amazon S3 via VPN.

AWS SAA-C01 Question feedback

Question : 5 of 15 - Multiple Choice — Graded

Your Auto Scaling group is configured to launch one new Amazon EC2 instance if the overall CPU load exceeds 65% over a five-minute interval. Occasionally, the Auto Scaling group launches a second Amazon EC2 instance before the first is operational. The second instance is not required and introduces needless compute costs. How can you prevent the Auto Scaling group from launching the second instance?

Incorrect — Time spent : 9 sec

Your answer

A. Configure a lifecycle hook for your Auto Scaling group
B. Add a scaling-specific cooldown period to the scaling policy
C. Adjust the CPU threshold that triggers a scaling action
D. Attach a new launch configuration to the Auto Scaling group

Correct Answer

B. Add a scaling-specific cooldown period to the scaling policy

Explanation

Correct answer is **B** as you need to adjust the cool down period for the newly added instance to startup and handle traffic.

Refer AWS documentation - Auto Scaling Cooldowns

The Auto Scaling cooldown period is a configurable setting for your Auto Scaling group that helps to ensure that Auto Scaling doesn't launch or terminate additional instances before the previous scaling activity takes effect. After the Auto Scaling group dynamically scales using a simple scaling policy, Auto Scaling waits for the cooldown period to complete before resuming scaling activities. When you manually scale your Auto Scaling group, the default is not to wait for the cooldown period, but you can override the default and honor the cooldown period. If an instance becomes unhealthy, Auto Scaling does not wait for the cooldown period to complete before replacing the unhealthy instance.

AWS SAA-C01 Question feedback

Question : 6 of 15 - Multiple Choice — Graded

A company is building software on AWS that requires access to various AWS services. Which configuration should be used to ensure that AWS credentials (i.e., Access Key ID/Secret Access Key combination) are not compromised?

Incorrect — Time spent : 9 sec

Your answer

A. Enable Multi-Factor Authentication for your AWS root account.
B. Assign an IAM role to the Amazon EC2 instance
C. Store the AWS Access Key ID/Secret Access Key combination in software comments.
D. Assign an IAM user to the Amazon EC2 Instance.

Correct Answer

B. Assign an IAM role to the Amazon EC2 instance

Explanation

Correct answer is **B** as IAM role can be used by EC2 instance to access other AWS services, which help generate temporary short lived credentials

Refer AWS documentation - IAM Role

An IAM role is similar to a user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have any credentials (password or access keys) associated with it. Instead, if a user is assigned to a role, access keys are created dynamically and provided to the user.

Option A is wrong as MFA is to enable two factor authentication

Option C is wrong as storing credentials is not recommended

Option D is wrong as IAM user cannot be assigned to EC2 instance

AWS SAA-C01 Question feedback

Question : 7 of 15 - Multiple Choice — Graded

A web application allows customers to upload orders to an S3 bucket. The resulting Amazon S3 events trigger a Lambda function that inserts a message to an SQS queue. A single EC2 instance reads messages from the queue, processes them, and stores them in a DynamoDB table partitioned by unique order ID. Next month traffic is expected to increase by a factor of 10 and a Solutions Architect is reviewing the architecture for possible scaling problems. Which component is MOST likely to need re-architecting to be able to scale to accommodate the new traffic?

Incorrect — Time spent : 7 sec

Your answer

A. Lambda function
B. SQS queue
C. EC2 instance
D. DynamoDB table

Correct Answer

C. EC2 instance

Explanation

Correct answer is **C** as a single EC2 instance is not scalable and the architecture needs to be improved using Auto Scaling to scale up or down as the demand changes.

Option B and D are AWS managed services and scale as per the configuration and demand.

Option A is wrong as Lambda function scales as per the incoming demand.

AWS SAA-C01 Question feedback

Question : 8 of 15 - Multiple Choice — Graded

A customer wants to track access to their Amazon Simple Storage Service (S3) buckets and also use this information for their internal security and access audits. Which of the following will meet the Customer requirement?

Incorrect — Time spent : 5 sec

Your answer

A. Enable AWS CloudTrail to audit all Amazon S3 bucket access.
B. Enable server access logging for all required Amazon S3 buckets
C. Enable the Requester Pays option to track access via AWS Billing
D. Enable Amazon S3 event notifications for Put and Post.

Correct Answer

B. Enable server access logging for all required Amazon S3 buckets

Explanation

Correct answer is **B**

In order to track requests for access to your bucket, you can enable access logging. Each access log record provides details about a single access request, such as the requester, bucket name, request time, request action, response status, and error code, if any. Access log information can be useful in security and access audits

Refer to AWS documentation for S3 Server logs

Option A is wrong as CloudTrail would only give information for the API calls to S3 and not the individual access information

Option C is wrong as it only helps handle billing if you want the user to pay for the object access

Option D is wrong as event notifications does not cover all the information

AWS SAA-C01 Question feedback

Question : 9 of 15 - Multiple Choice — Graded

You have EC2 instances in three availability zones, with a load balancer configured on all the three AZs. You observe that one availability zone is receiving more traffic as compared to other AZs, how can you solve this problem effectively

Correct — Time spent : 21 sec

Your answer

A. Disable sticky sessions
B. Reduce the frequency of the health checks
C. Enable cross zone load balancer
D. Amazon recommends to use two availability zone behind ELB

Correct Answer

A. Disable sticky sessions

Explanation

Correct answer is **A** asSticky Sessions may cause the users to be routed to the same instances.

Option B is wrong as reducing frequency of health checks would only help determining whether the instance is healthy or not. And it would be the same for all the instances across AZs.

Option C is wrong as enabling cross zone load balancer would only help route traffic equally across instances and not the AZs, which seems not to be the case here.

Option D is wrong as AWS recommends spreading you instances across all available AZs to make the application HA

AWS SAA-C01 Question feedback

Points : 3 out of 3

Question : 10 of 15 - Multiple Choice — Graded

How can you secure data at rest on an EBS volume?

Incorrect — Time spent : 13 sec

Your answer

A. Encrypt the volume using the S3 server-side encryption service
B. Attach the volume to an instance using EC2's SSL interface.
C. Create an IAM policy that restricts read and write access to the volume.
D. Use EBS encryption
E. Use an encrypted file system on top of the EBS volume

Correct Answer

D. Use EBS encryption

Explanation

Correct answer is **D** as EBS encryption can be used to encrypt EBS volumes.

EBS encryption was launched some time back by AWS. Before the EBS encryption, Option E was the correct answer, as you need to use encrypted file system over EBS volume.

Until today, you needed third-party security tools to encrypt data for EBS volumes. With Amazon EBS encryption, you can now create an encrypted EBS volume and attach it to a supported instance type. Data on the volume, disk I/O, and snapshots created from the volume are then all encrypted. The encryption occurs on the servers that host the EC2 instances, providing encryption of data as it moves between EC2 instances and EBS storage. EBS encryption is based on the industry standard AES-256 cryptographic algorithm.

Option A is wrong as S3 - SSE does not work with EBS.

Option B is wrong as SSL is for data in transit.

Option C is wrong as IAM policy can't restrict read & write access to EC2.

AWS SAA-C01 Question feedback

Question : 11 of 15 - Multiple Choice — Graded

A client application requires operating system privileges on a relational database server. What is an appropriate configuration for highly available database architecture?

Incorrect — Time spent : 13 sec

Your answer

A. A standalone Amazon EC2 instance
B. Amazon RDS in a Multi-AZ configuration
C. Amazon EC2 instances in a replication configuration utilizing a single Availability Zone
D. Amazon EC2 instances in a replication configuration utilizing two different Availability Zones

Correct Answer

D. Amazon EC2 instances in a replication configuration utilizing two different Availability Zones

Explanation

Key point here is to design a HA solution Database solution with operating system privileges.

Correct answer is **D** as RDS is a managed service from AWS and it does not provide operating system privileges and for HA there need to be instances in at least 2 AZs

Option A is wrong as single instance does not provide HA

Option B is wrong as RDS does not provide operating system privileges.

Option C is wrong as single AZ does not provide HA

AWS SAA-C01 Question feedback

Question : 12 of 15 - Multiple Choice — Graded

You have an application running on an Amazon Elastic Compute Cloud instance, that uploads 5 GB video objects to Amazon Simple Storage Service (S3). Video uploads are taking longer than expected, resulting in poor application performance. Which method will help improve performance of your application?

Incorrect — Time spent : 12 sec

Your answer

A. Enable enhanced networking
B. Use Amazon S3 multipart upload
C. Leveraging Amazon CloudFront, use the HTTP POST method to reduce latency.
D. Use Amazon Elastic Block Store Provisioned IOPS and use an Amazon EBS-optimized instance

Correct Answer

B. Use Amazon S3 multipart upload

Explanation

Correct answer is **B as** Multipart upload allows you to upload a single object as a set of parts and in parallel. Each part is a contiguous portion of the object's data. You can upload these object parts independently and in any order. If transmission of any part fails, you can retransmit that part without affecting other parts. After all parts of your object are uploaded, Amazon S3 assembles these parts and creates the object. In general, when your object size reaches 100 MB, you should consider using multipart uploads instead of uploading the object in a single operation.

Refer to AWS documentation for S3 Multipart upload

Option A & D is wrong as enhanced networking, IOPS, EBS optimized helps improve the performance within the AWS network for the EC2 instances

Option C is wrong as CloudFront allows uploading objects from global locations a bit smoother but would not improve the S3 upload time

AWS SAA-C01 Question feedback

Question : 13 of 15 - Multiple Choice — Graded

You have been asked to architect a file system for user's home directories. The solution must be accessible simultaneously to individuals across an organization. Users and groups must have permissions defined at the file or directory level. What AWS service can meet all of these requirements?

Incorrect — Time spent : 18 sec

Your answer

A. Amazon EBS
B. Amazon S3
C. Amazon EFS
D. Amazon DynamoDB

Correct Answer

C. Amazon EFS

Explanation

Correct answer is **C** as EFS is ideal solution to create user home directories and accessible across individuals across organizations, with the ability to configure it.

Refer AWS EFS FAQs & Create Writable Per-User directories

Q. What use cases is Amazon EFS intended for?

Amazon EFS is designed to provide performance for a broad spectrum of workloads and applications, including Big Data and analytics, media processing workflows, content management, web serving, and home directories.

AWS SAA-C01 Question feedback

Question : 14 of 15 - Multiple Choice — Graded

Your company is running an online sale over the coming weekend, and you will need additional compute resources to carry the additional load. If the availability of these additional instances must be guaranteed for the duration of the sale, what is the most cost-effective EC2 pricing option for this job?

Correct — Time spent : 6 sec

Your answer

A. On-Demand Instances
B. Spot Instances + On-Demand Instances
C. Reserved Instances (3 year contract)
D. Dedicated Instances

Correct Answer

A. On-Demand Instances

Explanation

Correct answer is **A** as On Demand instances would help provision extra capacity with the availability of these additional instances guaranteed as compared to the Spot instances.

Refer AWS documentation - EC2 Purchasing Options

Option B is wrong as Spot instances might be cost effective but does not guarantee availability

Option C is wrong as using Reserved instances is not cost effective

Option D is wrong as Dedicated instances just provided isolated hardware separated from other clients and has most cost.

AWS SAA-C01 Question feedback

Points : 3 out of 3

Question : 15 of 15 - Multiple Answer — Graded

A company is preparing to give AWS Management Console access to developers. Company policy mandates identity federation and role-based access control. Roles are currently assigned using groups in the corporate Active Directory. What combination of the following will give developers access to the AWS console? Choose 2 answers

Incorrect — Time spent : 8 sec

Your answer

A. AWS Directory Service AD Connector
B. AWS Directory Service Simple AD
C. AWS Identity and Access Management groups
D. AWS Identity and Access Management roles
E. AWS Identity and Access Management users

Correct Answer

A. AWS Directory Service AD Connector
D. AWS Identity and Access Management roles

Explanation

Correct answer are **A & D** as AD connector is required to connect to on-premises Active Directory and IAM Role can be used for Identity Provider and Federation.

Refer AWS blog - How to connect on-premises active directory using AD Connector

AD Connector is a directory gateway with which you can redirect directory requests to your on-premises Microsoft Active Directory without caching any information in the cloud

Your end users and IT administrators can use their existing corporate credentials to log on to AWS applications such as Amazon WorkSpaces, Amazon WorkDocs, or Amazon WorkMail.

You can manage AWS resources like Amazon EC2 instances or Amazon S3 buckets through IAM role-based access to the AWS Management Console.

Option B is wrong as Simple AD is a standalone AD setup and does not allow connection to the on-premises AD.

Option C & E are wrong as users and groups do not work.

AWS SAA-C01 Question feedback

2/15 Questions right