AWS Certified Solutions Architect – Associate

You've been tasked with replicating your production VPC in another region for disaster recovery purposes. Part of your environment relies on EC2 instances with preconfigured software. What steps would you take to configure the instances in another region?

1. Create AMIs of the instances and copy them to the new Region for deployment.
2. Create AMIs of the instances and deploy them in the new Region
3. Write the IAM permissions for the new Region to use the AMIs from the original Region.
4. None of these.

EXPLANATION:

The AMIs must be copied to the new Region prior to deployment.

Answer: a

You are creating an RDS database for your production environment and it needs to be highly available and continue to function in the event of an outage to the Primary database. Which of the following options will best meet this requirement?

1. Multi-AZ deployment
2. Cross-region deployment
3. Read replicas
4. Multi-region deployment

EXPLANATION:

Multi-AZ deployment involves the creation of a standby replica in a different Availability Zone (AZ) from the primary database. A standby replica cannot serve read traffic, it is used to synchronously replicate data from the primary database. AZs are isolated from one another to prevent failure from spreading to them all. So, if the location of the primary database has issues, Amazon RDS automatically fails over to the standby replica. Read replicas are used to scale out to cater for high volumes of read requests - not automated failover. Multi-region deployment is not a valid RDS option and Cross-region deployments enable support for scaling of Read replicas and can be used for cross-region DR, but don't support the automatic failover due to a Primary DB outage.

Answer: a

You are reviewing Change Control requests and you note that there is a proposed change designed to reduce errors due to S3 Eventual Consistency by updating the 'DelaySeconds' attribute. What does this mean?

1. When the consumer instance polls for new work, the consumer instance will wait a certain time until it has a full workload before closing the connection.
2. While processing a message, a consumer instance can amend the message visibility counter by a fixed amount.
3. When a new message is added to the SQS queue, it will be hidden from consumer instances for a fixed period.
4. While processing a message, a consumer instance can reset the message visibility by restarting the preset timeout counter.

EXPLANATION:

Poor timing of SQS processes can significantly impact the cost effectiveness of the solution.

Answer: c

Your company stores confidential data in S3. To comply with regulations, the data needs to be made available in a different geographical location. What steps would you take to be within compliance?

1. Enable Cross-Region Replication for the S3 bucket.
2. Copy the data to an EBS volume in another region.
3. Create a snapshot of the S3 bucket and copy it to another region.
4. Apply Multi-AZ for the S3 bucket.

EXPLANATION:

This is a specific use case for S3 Cross-Region Replication. Comply with compliance requirements—Although Amazon S3 stores your data across multiple geographically distant Availability Zones by default, compliance requirements might dictate that you store data at even greater distances. Cross-region replication allows you to replicate data between distant AWS Regions to satisfy these requirements.

Answer: a

Which of the following are the application integration services enable communication between decoupled components in order to build a scalable and more resilient solution?

1. Amazon MQ
2. AWS Simple Email Service (SES)
3. Amazon Data Sync
4. Amazon App Sync
5. Amazon SQS

EXPLANATION:

Amazon SQS, Amazon MQ and Amazon App Sync are AWS application integration services. Application integration services enable communication between decoupled components within micro-services, distributed systems, and serverless applications so you can easily build scalable and more resilient solutions. Amazon DataSync is AWS Migration and Transfer service and is not an integration service. AWS SES is a cloud-based email sending service designed for customer engagement.

Answer: a, d, e

Even though your company is migrating to Amazon EC2, it wants to continue using its Oracle 12c software license to comply with the contract requirements of one of its clients. Which of the following pricing models accommodates this goal?

1. Reserved
2. Spot
3. On Demand
4. Dedicated Hosts

EXPLANATION:

Consisting of an actual physical EC2 server, the Dedicated Hosts plan will allow the company to use its eligible software license from Oracle on Amazon EC2. The other choices will not work because they don’t include a physical server to address corporate compliance requirements.

Answer: d

A company has an LNMP (Linux, Nginx, MySQL, PHP) stack application deployed to AWS. The availability requirements for their backend database specify automatic failover in case of disaster recovery. What is the optimal solution that meets this requirement?

1. RDS with Multi-AZ deployment.
2. RDS with Read-Replica deployment.
3. DynamoDB with Global Tables deployment.
4. Deploy multiple RDS instances. Use Route53 with Health-Check and DNS failover configured.

EXPLANATION:

Since the scenario calls for MySQL, we must choose a relational database for the backend database. This means that DynamoDB is not a correct option. With RDS Multi-AZ deployment, a primary DB instance is automatically and synchronously replicated to a secondary RDS instance in a different availability zone (AZ). In case of a disaster causing primary instance failure, RDS performs automatic failover to the secondary standby RDS instance. During the failover, the database endpoint remains the same. RDS Read-Replica provide secondary RDS instances that are asynchronous replicated from the primary. RDS read-replicas have different endpoints and do not provide automatic failover. Additionally, they only provide read (not write) operations. It is possible to use Route53 with Health-check and DNS failover configurations to route traffic to multiple RDS instances. However, this solution does not provide automatic data synchronization between instances.

Answer: a

Your company is planning on moving to AWS. One of your applications will be launched on a set of EC2 instances. You will need to ensure that the architecture is fault tolerant and highly available. Which of the following would be considered during the design process?

1. Use a load balancer in front of the EC2 instances.
2. Ensure that the EC2 instances are spread across multiple Availability Zones.
3. Ensure that the EC2 instances are spread across a single Availability Zone for better maintenance.
4. Enable Multi-AZ for the databases.

EXPLANATION:

Most of the higher-level services, such as Amazon Simple Storage Service (S3), Amazon SimpleDB, Amazon Simple Queue Service (SQS), and Amazon Elastic Load Balancing (ELB), have been built with fault tolerance and high availability in mind. Services that provide basic infrastructure, such as Amazon Elastic Compute Cloud (EC2) and Amazon Elastic Block Store (EBS), provide specific features, such as availability zones, elastic IP addresses, and snapshots, that a fault-tolerant and highly available system must take advantage of and use correctly. Just moving a system into the cloud doesn’t make it fault-tolerant or highly available.

Answer: a, b

If an instance belonging to an Elastic Load Balancer fails its health check, what will the ELB do?

1. The ELB will launch a new instance.
2. ELB will tell Auto Scaling to launch a new instance.
3. The ELB will de-register the instance and stop sending traffic to it.
4. Unfortunately, the ELB will continue to send the unhealthy instance traffic until the instance is terminated.

EXPLANATION:

The ELB will de-register the instance and stop sending traffic to it.

Answer: c

An enterprise is looking to implement Amazon SQS as a messaging service to integrate multiple application components which are hosted in AWS. Which of the following are true about Amazon SQS?

1. Data transfer cost between Amazon SQS and Amazon EC2 or AWS Lambda within a single region incur a standard data transfer rate.
2. Amazon SQS stores all messages and message queues within a single highly-available AWS region with multiple redundant Availability Zones.
3. Amazon SQS stores all messages and message queues across several highly-available AWS regions with multiple redundant Availability Zones.
4. Amazon SQS stores all messages and message queues within single AWS region within an Availability Zone.
5. Data transfer cost between Amazon SQS and Amazon EC2 or AWS Lambda within a single region is free.

EXPLANATION:

Amazon SQS stores all messages within a region and can store messages across AZs within the region. Data transfer between Amazon SQS and Amazon EC2 or AWS Lambda within a single region is free.

Answer: b, e

A Fortune 500 company is currently migrating to AWS. The organization has determined that it needs an AWS Support plan that can mitigate failure or disruption of processes essential to its operation. Which of the following plans is most suitable for this purpose?

1. Business
2. Developer
3. Basic
4. Enterprise

EXPLANATION:

Basic Support is included with each AWS account, so that automatically rules it out as the correct answer. Based on the description of the company’s needs and size, Enterprise Support is strongly recommended. This plan is ideally designed for organizations that have business or mission-critical workloads in AWS. Developer is geared towards those who experiment or test in AWS, and Business is ideal for production workloads. Neither of them is as robust as the Enterprise offering.

Answer: d

You are discussing the needs for a new Oracle DB server. The database routinely consumes about 15,000 IOPS, but can easily reach 20,000 during peak periods. There is also concern that the storage will need to be at least as durable, if not more, than a traditional on-premise physical magnetic disk, leading to discussions on if RAID-10 is required. What design decisions would you recommend?

1. Use SSD Instance Stores configured as RAID-10. This will exceed the performance rate and the RAID-10 configuration will protect against all likely data loss.
2. Use gp2 EBS storage. It will deliver 16,000 IOPS and can use the burst capability to cover higher demand spikes.
3. Use io1 EBS storage. It can be tuned to deliver the performance needed by the DB server.
4. EBS virtual volumes offer higher reliability than the stated requirement, so RAID adds little advantage, and much complication.
5. EBS virtual volumes offer less reliability than the stated requirement. Given the critically of the server a RAID-10 configuration is a good idea.

EXPLANATION:

Data stored on EBS volumes is automatically and redundantly stored in multiple physical volumes in the same availability zone as part of the normal operations of the EBS service at no additional charge. gp2 will deliver up to 16,000 IOPS, however there will be no burst capacity above that. Instance Store storage can provide very high performance, however it is ephemeral, and extra precautions would be needed to ensure recovery in teh event that the instance itself failed.

Answer: c, d

You are a system administrator and you need to take a consistent snapshot of your EC2 instance. Your application holds large amounts of data in cache that is not written to disk automatically. What would be the best approach to taking an application consistent snapshot?

1. Shut down the EC2 instance and detach the EBS volume, then take the snapshot.
2. Take a snapshot using the AWS CLI.
3. Take a snapshot in real time using the EC2 API.
4. In the AWS console, take a snapshot and ensure that the 'application consistent' check box is ticked.

EXPLANATION:

As you need an application consistent snapshot, your best option would be to shutdown the EC2 instance and detach the EBS volume, then take the snapshot.

Answer: a

You are a solutions architect working for a company that conducts surveys on specific industries. Each industry that you survey has its own EC2 fleet, separate from those of other industries. Company policy dictates that you should keep costs to a minimum, using only 1 load balancer, if possible. What type of load balancer should you use to suit this requirement?

1. Elastic Load Balancer with IDS
2. Elastic Load Balancer with IPS
3. Classic Load Balancer
4. Application Load Balancer

EXPLANATION:

You need an application-aware load balancer, so your best option would be to use an Application Load Balancer.

Answer: d

You are using a classic elastic load balancer for a small website in order to save money. The classic load balancer is deployed in US-EAST-1A and it is supposed to distribute traffic to 3 EC2 instances, each in different Availability Zones. However when you check the logs you notice that only the EC2 instance in US-East-1A is receiving traffic. What could be the cause?

1. The load balancing algorithm needs content meta-data. You should upgrade the load balancer to an application load balancer in order to get layer 7 visibility.
2. You need to enable cross zone load balancing.
3. You need to enable sticky sessions.
4. The site is operating on Layer 4 and needs a static IP address, therefore you should upgrade your load balancer to a Network Load Balancer.

EXPLANATION:

For the Classic ELB, cross zone load balancing is a option.

Answer: b

The large manufacturing company you work for is interested in moving their production estate to AWS. They run a Joomla store which utilizes MySQL on the back end. Currently, they also use clustered MySQL databases in an active/passive configuration at a single site. In moving to AWS, they want an active/passive configuration across 2 geographically distinct locations, with automatic failover between the two. As their solutions architect, which of the following RDS options should you recommend?

1. RDS with Cross Region Failover
2. RDS Multi-AZ
3. RDS with Cross Region Replication
4. RDS Read Replicas

EXPLANATION:

To automatically failover from one geographic location to another you should use Multi-AZ for RDS.

Answer: b

You have a web application that serves different data to users based on their location. To do this, you are using Geolocation Routing to redirect users to the appropriate load balancer depending on their location around the globe. This seems to work well for most, however you have been getting reports of some users not being able to resolve your DNS address. What is the most likely cause of this?

1. They need to configure their system to use AWS's DNS servers for DNS resolution
2. They are running anonymity software that is hiding their IP address
3. You have not created a "NoRegion" record
4. You have not created a "Default" record

EXPLANATION:

If a user is coming in from a region for which you have not created a record for, or if AWS is not able to identify the region the user is coming in from by their IP, AWS will return whatever appears in the "Default" record. If no "Default" record is created, the user will receive a "no answer" response from AWS, and not be able to resolve the address to your application. There is no such thing as the "NoRegion" record type. Although anonymity software may obfuscate the user's IP, the anonymity provider's IP will still be exposed and used to geo-route the user. This may mean they are served content not appropriate for their region, but DNS resolution will still work as intended. There is no need to configure user systems to use AWS's DNS servers, as the user's DNS servers will forward the request to AWS DNS servers automatically as needed.

Answer: d

The dashboard application for multiple company contact centers requires fast update response times for a large number of concurrent users. Call center metric data is stored in an Oracle version 11 database. Which architecture will provide high-availability and the low response times needed for this mission-critical data?

1. Oracle hosted on Amazon EC2 in Multiple Availability Zones with EBS snapshots
2. Oracle hosted on Amazon EC2 in multiple Availability Zones with Oracle Data Guard replication
3. An Amazon RDS Oracle Instance with AWS Database Replication Service
4. An Amazon RDS Oracle instance with Multi-AZ and Read Replicas

EXPLANATION:

Since the dashboard updates are needed across multiple contact centers, leveraging read-only replicated databases will provide fast response times. Amazon RDS doesn’t support read replicas for Oracle version 11, so hosting the database on EC2 and replicating the data with Oracle Data Guard is the only viable solution. AWS Database Replication Service is not an offered service, and using EBS snapshots won't provide real-time replication.

Answer: b

In the future, you will need to preserve, restore, and retrieve every version of every file that you have stored in AWS. Which service should you use?

1. S3 with Versioning enabled.
2. RDS
3. S3 - OneZone-IA
4. Glacier

EXPLANATION:

Versioning allows you to preserve, retrieve, and restore every version of every object stored in an Amazon S3 bucket.

Answer: a

A company's SOC is implementing a system to perform real-time analysis of CloudTrail logs to enhance their security. What option would enable them to receive logs from CloudTrail in real-time in the most optimal way?

1. Create a Kinesis Stream. Configure the CloudTrail trail to send notifications to the Kinesis Stream. Use Kinesis Data Analytics to perform analysis on the data.
2. Create a Kinesis Stream. Configure the CloudTrail S3 bucket notifications with the Kinesis stream as the message destination. Implement a Lambda function to process messages from the Kinesis Stream.
3. Configure CloudWatch Events rule that is triggered when new logs are written to CloudTrail. Implement a Lambda function to analyse the event. Configure the Lambda function as the CloudWatch Event target.
4. Create an SNS Topic. Configure the CloudTrail trail to send notifications to the SNS Topic. Configure SQS Queue to subscribe to the SNS Topic.

EXPLANATION:

CloudTrail can be configured to send notifications to an SNS topic. SQS Queue can be configured to subscribe to the SNS topic so that messages can be processed programmatically. S3 notifications do not have ability to send messages to Kinesis Streams, so this is not a valid option. Likewise, CloudTrail does not have ability to send notification to Kinesis Streams. Using CloudWatch Events rules as a trigger is not an operationally optimal solution since CloudTrail has native notification capability.

Answer: d

Which of the below services create entities that only exist in the region that they are created in by default?

1. Route 53
2. EC2
3. DynamoDB
4. SNS
5. S3
6. VPC
7. IAM
8. CloudFront

EXPLANATION:

IAM, SNS, Route 53 and CloudFront are all global services, with in-built redundancy, these entities are available in all regions. VPC and DynamoDB store all their entities and data in a redundant fashion in the region they were created in, and EC2 stores the data and objects in the AZ it was created in. S3 is a little more tricky - although it can be seen as a "Global" service as data can be accessed from anywhere, that data only exists in the region that the bucket was created in by default

Answer: b, c, e, f

Which of the following components are not part of Amazon ECS?

1. File Storage
2. Task Scheduling
3. Service Discovery
4. Task Definitions

EXPLANATION:

Service Discovery makes it easy for containers within an ECS cluster to discover and connect with each other, using Route 53 endpoints. Task Definitions define the resource utilisation and configuration of tasks, using JSON templates. Task Scheduling allows you to run batch processing jobs run on a schedule. File Storage is not a component of ECS. Storage within ECS is handled by EBS volumes attached to the underlying EC2 instances and not by ECS itself.

Answer: a

Which of the following are ways of automating your RDS backups?

1. Automated Snapshots
2. Automated Backups
3. Using Data Pipeline
4. Using S3

EXPLANATION:

Amazon RDS provides two different methods for backing up and restoring your DB Instance(s): automated backups and database snapshots.

Answer: a, b

To maintain compliance with HIPAA, all healthcare-related data being stored on Amazon S3 needs to be encrypted at rest. Assuming S3 is being used for storing the data, which of the following are the preferred methods of encryption?

1. Encrypt the data locally using your own encryption keys and then transfer the encrypted data to S3.
2. Store the data in S3 as EBS snapshots.
3. Store the data on encrypted EBS volumes.
4. Enable Server Side Encryption on your S3 bucket. S3 automatically applies AES-256 encryption.

EXPLANATION:

You could encrypt locally or let S3-SSE handle encryption for you. Local encryption will generally cost more due to overhead, testing and management not required if you use the certified S3 offering.

Answer: a, d

The marketing department at your company wants to run a Hadoop cluster on Amazon EMR to perform data mining on a 2 TB dataset. Your information security group requires that all data be encrypted in transit and at rest, both on-premises and in the cloud at all times. Encryption keys must be stored in the on-premises key management solution. You've decided to transmit the data to Amazon S3 using TLS. How will you protect the data at rest for processing by the EMR cluster?

1. Use the AWS SDK for Java to implement the encryption materials provider interface in the EMRFS client. Retrieve the key from the on-premises key management system to decrypt the data stored in S3
2. Specify server-side encryption when you create the S3 bucket where the data will be uploaded. Decrypt the data before uploading it into S3 and let S3 manage encryption and decryption going forward
3. Specify client-side encryption when you create the S3 bucket where the data will be uploaded. Configure S3 to use the on-premises key management system. Let S3 handle decryption for EMR
4. Load the on-premises encryption key into AWS Key Management Service as an AWS Managed Customer Master Key. In the EMRFS client, retrieve the key from KMS to decrypt the data stored in S3

EXPLANATION:

With S3 client-side encryption, the S3 decryption needs to take place in the EMRFS client on your cluster. In this case, since the data was encrypted with on-premises keys before being uploaded to S3, we need to retrieve those keys using the custom key provider capabilities provided by the AWS SDK for Java. Once the keys are retrieved in the EMRFS client, we can decrypt the S3 data. You can't load an AWS Managed Customer Master Key into KMS. AWS Managed CMKs are created, managed, and used on your behalf by AWS services that are integrated with KMS. KMS does provide the capability to load Customer Managed CMKs. S3 currently doesn't allow you to specify a key management system other than AWS KMS for encryption. Decrypting the data and letting S3 re-encrypt it will work with SSE-S3, but it will require significant additional processing.

Answer: a

Which of the following layers of DDoS attacks does AWS automatically address?

1. Layer 4
2. Layer 1
3. Layer 3
4. Layer 7

EXPLANATION:

AWS automatically addresses DDoS attacks at the network and transport layers, which are Layer 3 and Layer 4, respectively.

Answer: a, c

You have an EC2 instance with a Security Group attached. This security group is configured to only allow inbound traffic from 192.168.0.0/24. A colleague has also configured a NACL on the subnet that the instance resides on, and this NACL is configured to block all traffic, except where the source or destination is in 192.168.0.0/24. What will happen when an instance with an IP of 192.168.1.12 tries to connect to your instance on port 80?

1. The security group will block the traffic before it is evaluated by the NACL
2. The traffic will be blocked simultaneously by the Security Group and NACL
3. The traffic will be allowed as it is still within a private range
4. The NACL will block the traffic before it is evaluated by the security group

EXPLANATION:

With inbound traffic, NACLs are evaluated before Security Groups. As the NACL is configured to only allow traffic from 192.168.0.0/24 and the IP 192.168.1.12 does not fall within that range, it will be blocked by the NACL before reaching the Security Groups.

Answer: d

You are currently running an application in a production environment and you want to ensure that it is free of vulnerabilities. Which of the following AWS services would you use to accomplish this?

1. AWS Web Application Firewall (WAF)
2. Amazon Inspector
3. AWS Trusted Inspector
4. AWS Shield

EXPLANATION:

You will need Amazon Inspector to perform a security assessment. Not only does it identify vulnerabilities in your application, it will also spot deviations from security best practices. AWS Shield and WAF protect the application from attacks that exploit vulnerabilities, rather than identify them. And Trusted Advisor only provides recommendations on how to improve security.

Answer: b

You've been tasked with the implementation of an offsite backup/DR solution. You'll only be responsible only for flat files and server backup. Which of the following would you include in your proposed solution?

1. Storage Gateway
2. S3
3. EC2
4. Snowball

EXPLANATION:

EC2 is a compute service not directly applicable to this providing backups. All others could be part of a comprehensive backup/DR solution.

Answer: a, b, d

To establish a successful site-to-site VPN connection from your on-premise network to an AWS Virtual Private Cloud, which of the following must be configured?

1. A NAT instance
2. A Virtual Private Gateway
3. An on-premise Customer Gateway
4. A private subnet in your VPC
5. A VPC with Hardware VPN Access

EXPLANATION:

You must have a VPC with Hardware VPN Access, an on-premise Customer Gateway, and a Virtual Private Gateway to make the VPN connection work.

Answer: b, c, e

Your organization currently has 2 VPCs in the same region - VPC A which has been configured with the subnet 10.1.0.0/16 and VPC B which has been configured with the subnet 10.1.250.0/24. A new requirement has come up to allow all resources in VPC A to access all resources in VPC B and vice versa. One of your colleagues has suggested that you peer the two VPCs together to accomplish this - what is your opinion on this?

1. Peering these two VPCs sounds like a good plan
2. You will need to deploy an NAT instance before the VPCs can be peered
3. You will need to use VPC Endpoint to peer the two VPCs
4. This will not be possible with the current configuration

EXPLANATION:

As the two VPCs have overlapping IP Address ranges, peering will not be possible. VPC Endpoints and NAT Instance will be of no use in peering these two VPCs. The "easiest" way forward to accomplish this would be to re-IP the resources in VPC B with a non-overlapping subnet, then peering the two

Answer: d

Your mobile app needs to have images uploaded to S3. You want to bypass the existing web server for the uploads to avoid increasing load on the server. How can this be accomplished?

1. Use Pre-Signed URLs to upload the images.
2. Use ECS Containers to upload the images.
3. Create a second S3 bucket and use Lambda to sync the files to the primary bucket.
4. Upload the images to SQS and then push them to the S3 bucket.

EXPLANATION:

All objects and buckets by default are private. The pre-signed URLs are useful if you want your user/customer to be able to upload a specific object to your bucket, but you don't require them to have AWS security credentials or permissions.

Answer: a

You must encrypt all incoming and outgoing traffic between your AWS environment and your customers. Your fleet of EC2 instances lives inside a public subnet and behind an elastic load balancer. Your application is very CPU intensive, and you want to minimize the processing load these EC2 instances must bear. What should you do?

1. Configure a NAT and install the EC2 instance on that NAT so that you offload SSL termination to a third party EC2 instance and not your production environment.
2. Install the SSL certificates on each EC2 instance and allow them to do the encryption/decryption with your customers.
3. Install the SSL certificates on your ELBs so that there is less load on the EC2 instances.
4. Use API Gateway to offload the SSL certificate, reducing the amount of load on both your ELB and EC2 instances.

EXPLANATION:

The best answer would be to offload your SSL decryption to an Elastic Load Balancer.

Answer: c

You want to enable EC2 instances in your AWS environment to download software updates over HTTP (Port 80) from the internet. What Security Group settings will enable this?

1. Inbound: Allow HTTP (Port 80) from 0.0.0.0/0 Outbound: HTTP (Port 80) to 0.0.0.0/0
2. Outbound: Allow HTTP (Port 80) to 0.0.0.0/0
3. Inbound: Allow ALL Ports from 0.0.0.0/0, Outbound: Allow HTTP (Port 80) to 0.0.0.0/0
4. Inbound: Allow HTTP (Port 80) from 0.0.0.0/0
5. Inbound: Allow HTTP (Port 80) from 0.0.0.0/0 Outbound: HTTP (Port 80) to IP address of Software Repo

EXPLANATION:

Security Groups are stateful, so you only need to define the Outbound rule in the Security Group for this example as the EC2 instance is initiating the connection. Answers with inbound rules are incorrect, which leaves the answer with the Outbound rule allowing HTTP to 0.0.0.0/0. Once the EC2 instance has established valid HTTP connection with an Internet service, the target systems response is allowed.

Answer: b

You want to encrypt the data in your S3 buckets. You intend on managing the encryption keys and using Amazon S3 to manage the encryption itself. Which of the following S3 encryption types support your requirements?

1. Server-Side Encryption
2. Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
3. Server-Side Encryption with AWS Key Management Service (SSE-KMS)
4. Server-Side Encryption with Customer-Provided Keys (SSE-C)

EXPLANATION:

Although Response A is correct in a general sense, the question is asking for a specific type of server-side encryption. SSE-C is what you need if you want to manage the encryption keys and have Amazon manage the encryption. Both SSE-S3 and SSE-KMS support the management of keys, which does not match the requirements of this application.

Answer: d

How can you securely upload or download your data to/from the S3 service?

1. Via SSL endpoints using the HTTPS protocol
2. Via HTTP endpoints using the HTTP protocol
3. Via SSL endpoints using the HTTP protocol
4. Via TLS endpoints using the HTTPS protocol

EXPLANATION:

You can securely upload/download your data to/from Amazon S3 via SSL or HTTP endpoints using HTTPS.

Answer: a

By default, how many Elastic IP addresses are you limited to per region?

1. 20
2. 5
3. 15
4. 10

EXPLANATION:

By default, all accounts are limited to 5 Elastic IP addresses per region.

Answer: b

As a follow up to a recent security breach you have been asked what steps can be taken to ensure that System Administrators aways use signed communication when interacting with your AWS account via the API interface. Which statements are most accurate?

1. All http requests to the API must be manually signed via the process documented by AWS.
2. It will be necessary to install signing utilities provided by openssl.org to generate personalized signing certificates signed by the Secret key downloaded from IAM.
3. AWS advise against signing HTTP API traffic as the capability is redundant when communicating with the AWS API.
4. You must advise that this is an area over which customers have little control. The signing of all but anonymous requests is enforced by AWS.
5. The process of manually signing requests is only needed when writing bespoke low level connections with the API.

EXPLANATION:

AWS use the signing hash to identify the requester. The signing hash is unique and is generated from the access key ID and secret access key downloaded from IAM.

Answer: d, e

The company you work for is considering a move to AWS, but they are concerned that their current, 50Mbps connection will not be able to handle the 100 TB of data that need to be migrated without causing unacceptable downtime. As their solutions architect, which AWS service would you recommend to move this data?

1. S3 with Transfer Acceleration
2. Snowball
3. DirectConnect
4. AWS Storage Gateway

EXPLANATION:

Given the amount of data to be moved and the speed of the connection, Snowball would be the fastest and most economical solution.

Answer: b

Which of the following AWS services store data as key-value pairs?

1. S3
2. EC2
3. RDS
4. DynamoDB

EXPLANATION:

Both DynamoDB and S3 use key-value pairs.

Answer: a, d

You have designed an application that stores large videos in S3. These videos are usually larger than 100Mb in size. You need to maximize upload performance. Which of the following will achieve this end.

1. Design the application to use multipart upload, so that the file is split in to multiple parts which are then uploaded simultaneously.
2. Implement a third party CDN solution.
3. Utilize S3 Transfer Acceleration.
4. Require the users to use Direct Connect in order to use to application so as to maximize the upload bandwidth.

EXPLANATION:

Multipart Upload is recommended for files greater than 100 Mb, and is required for files 5 GB or larger. S3 Transfer Acceleration is especially useful in cases where your bucket resides in a Region other than the one in which the file transfer was originated.

Answer: a, c

You have a data warehouse on AWS utilizing Amazon Redshift of 50 Tb. Your data warehouse is located in us-east-1 however you are opening a new office in London where you will be employing some data scientists. You will need a copy of this Redshift cluster in eu-west-2 for performance and latency considerations. What is the easiest way to manage this migration?

1. Order an AWS Snowball. Export the Redshift data to the Snowball and then ship the snowball from us-east-1 to eu-west-2. Load the data into Redshift in London.
2. Export the data to S3 using Data Pipeline and configure Cross Region Replication to an S3 bucket based in London. Use AWS lambda to import the data back to Redshift.
3. In the AWS console go in to Redshift and choose Backup, and then choose Configure Cross-Region Snapshots. Select Copy Snapshot and then choose the eu-west-2 region. Once successfully copied use the snapshot in the new region to create a new Redshift cluster from the snapshot.
4. Create a new redshift cluster in eu-west-2. Once provisioned use AWS data pipeline to export the data from us-east-1 to eu-west-2.

EXPLANATION:

Where AWS provides a service, it is wise to use it rather than trying to create a bespoke service. The AWS service will have been designed and tested to ensure robust and secure transfer taking into account key management and validation.

Answer: c

You have been tasked with implementing a globally accessible storage solution that will scale from a few terabytes (now) to an unknown, but significantly greater, volume of data in three years time. Which AWS service would best meet your current and projected storage needs?

1. RDS
2. EC2 with EBS
3. S3
4. DynamoDB

EXPLANATION:

Amazon S3 is highly scalable, secure storage for 'flat' files. S3 will scale to any projected volume of data. In this case, it's your best bet.

Answer: c

You have a small database workload with infrequent I/O. Which storage medium would the most cost-effective way to meet these requirements?

1. Amazon RDS Cold Storage
2. Amazon RDS Provisioned IOPS (SSD) Storage
3. Amazon RDS General Purpose (SSD) Storage
4. Amazon RDS Magnetic Storage

EXPLANATION:

The question is specific that you are evaluating for RDS. Cold Storage is not a valid option for RDS. of the three valid types for RDS, Magnetic is still the cheapest

Answer: d

Your CFO is after a ballpark estimate for the new customer-facing loyalty portal that you are currently designing and plan to host on AWS. She is particularly interested in all ongoing data transfer storage costs and wants to check her understanding of S3 pricing with you. Select all of her correct statements.

1. The total costs for data transfer out from S3 to CloudFront depend on the monthly volume of data, i.e a tiered pricing applies: The more data goes out, the more you save.
2. Data transfer into S3 from the Internet doesn't incur any costs
3. Transfers between S3 buckets or from Amazon S3 to EC2 within the same AWS Region are free.
4. Transferring up to one GB of data per month out of S3 to end customers over the public internet is free.
5. All S3 costs are based on the volume of data regardless of how it is handled.

EXPLANATION:

Data transferred into S3 is generally free of $/GB charges. However the PUT, POST, GET, HEAD, etc transactions to process the data do carry a small cost per 1000 transactions. The data transfer OUT from Amazon S3 normally attracts a $/GB cost, except transfers to CloudFront is currently free.

Answer: b, c, d

You are working on a research project for a healthcare insurer and your first task is to ingest 6 months of trial data collected by about 30 participating physicians around the country. Each data set is about 15 GB in size and contains protected health information. You are proposing to use S3 Transfer Acceleration for the data upload to an S3 bucket but a colleague raises some concerns about that. Which of the following statements are valid?

1. Most physicians have only about 40 to 50Mbps of available bandwidth. S3 Transfer Acceleration is therefore not a good option.
2. Because S3 Transfer Acceleration is not a HIPAA eligible service, you can't use it to transfer protected health information between the physicians and your Amazon S3 bucket.
3. The name of your bucket used for Transfer Acceleration must be DNS-compliant and must not contain periods ('.').
4. It will take a long time because S3 Transfer Acceleration does not support all bucket level features including multipart uploads.

EXPLANATION:

S3 TA supports all bucket level features including multipart uploads. AWS has expanded its HIPAA compliance program to include Amazon S3 Transfer Acceleration as a HIPAA eligible service. In general; if there are recurring transfer jobs, and there is more than 25Mbps of available bandwidth, and it will not take more than a week to transfer over the Internet, S3 Transfer Acceleration is an acceptable option.

Answer: c

Which AWS service should you use to host MySQL, MariaDB, Oracle, SQL Server, or PostgreSQL database where you do not need to manage the underlying operating system?

1. Aurora
2. RDS
3. EC2 with EBS
4. DynamoDB

EXPLANATION:

Amazon RDS is available on several database instance types - optimized for memory, performance or I/O - and provides you with six familiar database engines to choose from, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle, and Microsoft SQL Server.

Answer: b

You are considering moving an on-premise SQL Server cluster into AWS, using EC2 instances rather than RDS. You need to recommend the most suitable EBS volume type for the cluster to use, but also pair it with a suitable EC2 instance type. You know that the throughput must be good, but the most important thing is to maintain a consistent level of IOPS under normal load which can increase to a much higher level at busy times. Choose the best option from the following EC2 and EBS pairings.

1. Provisioned IOPS (io1) EBS volumes with X1e EC2 instances
2. Throughout Optimised (st1) EBS volumes with X1e EC2 instances
3. Provisioned IOPS (io1) EBS volumes with r5 EC2 instances
4. Throughout Optimised (st1) EBS volumes with c5 EC2 instances

EXPLANATION:

The question states that you require consistent IOPS which means the io1 Provisioned IOPS type is the best choice of the two EBS types available, and therefore the correct answer must have io1 as an option. Of the remaining two answers, either EC2 families would work. We know from experience that databases do utilise as much memory as is available, so choosing an r5 family is plausible, however we need to use our extended knowledge of EC2 families to know that X1e was specifically created to run high performance databases and the final answer will therefore contain an io1 EBS volume and the X1e EC2 option.

Answer: a

You have a production application that is on the largest RDS instance possible, and you are still approaching CPU utilization bottlenecks. You have implemented read replicas, ElastiCache, and even CloudFront and S3 to cache static assets, but you are still bottlenecking. What should your next troubleshooting step be?

1. You should implement database partitioning and spread your data across multiple DB Instances.
2. You have reached the limits of public cloud. You should get a dedicated database server and host this locally within your own data center.
3. You should consider using RDS Multi-AZ and using the secondary AZ nodes as read only nodes to further offset load.
4. You should provision a secondary RDS instance and then implement and ELB to spread the load between the two RDS instances.

EXPLANATION:

If your application requires more compute resources than the largest DB instance class or more storage than the maximum allocation, you can implement partitioning, thereby spreading your data across multiple DB instances.

Answer: a

What is the availability of S3 - IA?

1. 99.99%
2. 99%
3. 99.9%
4. 99.999999999%

EXPLANATION:

S3 - IA is 99.9% available. Do not confuse availability with durability.

Answer: c

Amazon RDS supports which of the following databases?

1. DB2
2. MariaDB
3. MySQL
4. Sybase

EXPLANATION:

Amazon RDS currently supports MySQL, MariaDB, PostgreSQL, Oracle, Microsoft SQL Server, and Amazon Aurora database engines.

Answer: b, c

Your existing on-premise servers rely on Memcached to provide memory object caching. If you were to move to AWS, how might you preserve this functionality?

1. ElastiCache
2. None of these
3. Install Memcached on EC2
4. Elastic MapReduce

EXPLANATION:

ElastiCache is a web service that makes it easy to set up, manage, and scale a distributed in-memory cache environment in the cloud. It provides a high-performance, scalable, and cost-effective caching solution, while removing the complexity associated with deploying and managing a distributed cache environment.

Answer: a

As a Solutions Architect, you advise on team planning activities. A team is building an application that must store persistent JSON data and be able to have an index. Data access must remain consistent if there is high traffic volume. What service should you recommend to the team?

1. Amazon DynamoDB
2. Amazon ElastiCache
3. AWS CloudFormation
4. Amazon Redshift

EXPLANATION:

Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. The data stored in DynamoDB is JSON format, making it the perfect data store for this requirement.

Answer: a

You want to publish the information you capture about the IP traffic going in and out of your network interface so that you can view the data. Which of the following AWS services would achieve this?

1. EC2 instance
2. S3 bucket
3. VPC Flow Logs
4. CloudWatch Logs

EXPLANATION:

The information you capture about the IP traffic going in and out of your network interface can be published either in an S3 bucket or as a CloudWatch log. VPC Flow Logs is actually the feature that enables the recording of the information in the first place, but not used to publish the data.

Answer: b, d

With Amazon S3, you created a single-page website promoting your YouTube series. However, you want to use a domain name instead of the S3 endpoint. Which of the following services will enable this?

1. Amazon Redshift
2. Route 53
3. Amazon Elastic Compute Cloud (EC2)
4. AWS Lambda

EXPLANATION:

You require a domain name service for this, which is Route 53. You will need to register a domain name of your choosing with Route 53 and create an Alias record that links to the S3 bucket endpoint to be used as the website address. AWS Lambda and EC2 are compute services and Amazon Redshift is a Big Data and Data Warehouse service.

Answer: b

You have been load testing a customer’s new production environment. You create the environment using CloudFormation and you utilize CloudWatch to monitor the environment. After extensive load testing, you are ready to hand the CloudFormation template over to your customer. You delete the environment and give your customer the CloudFormation template. However, they now want to see the results of the load test. How long does CloudWatch store the metrics for EC2 & ELB after deleting those resources?

1. 24 months
2. 1 month
3. 15 months
4. 6 months

EXPLANATION:

CloudWatch stores metrics for terminated Amazon EC2 instances or deleted Elastic Load Balancers for 15 months.

Answer: c

You are developing a web application, and you are maintaining separate sets of resources for your alpha, beta, and release environments. Each version runs on Amazon EC2 with an EBS volume. You use Elastic Load Balancing to manage traffic and Amazon Route 53 to manage your domain. What's the best way to check the health and status of all three groups of services simultaneously?

1. Access CloudTrail audits for each set or resources.
2. Create a resource group containing each set of resources and view all three environments from a single, group dashboard.
3. Maintain an open console for each set of resources.
4. Use CloudWatch to proactively monitor each environment.

EXPLANATION:

With the Resource Groups tool, you use a single page to view and manage your resources.

Answer: b

An enterprise has both on-premise and AWS cloud applications and both are connected through a dedicated 10Gbps Direct Connect connection. The enterprise wants to manage this centrally and increase the connection bandwidth by utilizing Link Aggregation Group. Which of the following are true when considering LAG?

1. The maximum number of links is 4x in a LAG group
2. LAG Groups can be created with the same type of ports (either 1Gbps or 10Gbps)
3. There is no limitation on the number of links in a LAG group
4. LAG is available only for 1Gbps and 10Gbps Dedicated connection ports and is not available for Hosted Connections
5. A LAG group can be created with a mix of 1Gbps ports and 10Gbps ports

EXPLANATION:

Link Aggregation Groups (LAG) are a way for customers to order and manage multiple direct connect ports as a single larger connection instead of as separate discrete connections. The maximum number of links is 4x in a LAG group. LAG is available only for 1Gbps and 10Gbps Dedicated connection ports and is not available for Hosted Connections. LAG Groups can be created with the same type of ports (either 1Gbps or 10Gbps).

Answer: a, b, d

You have just deployed two EC2 instances into the public subnet of your default VPC - Web01 and Web02. These instances have been automatically allocated IPs of 10.0.0.15 and 10.0.0.16 respectively. You are trying to download some OS updates, but are having problems accessing internet resources from both VMs - even though they can see each other on the network. Which of the below is the MOST LIKELY cause of this scenario?

1. An Internet Gateway has not been deployed.
2. The instances have not been assigned an EIP
3. A NAT gateway has not been deployed
4. The instances do not have a valid private IP for the subnet.

EXPLANATION:

As the two instances can access each other, they already must have valid private IPs. AWS defines a "Public subnet" as one that has a Internet Gateway, plus a default route pointing to that Internet Gateway, so in this scenario one must already be in place. And, due to the fact that the default route in a public subnet always points to the Internet Gateway, deploying a NAT would be of little use. This leaves the lack of assigned EIPs as the most likely cause.

Answer: b

A financial services company is located in New York, while their development and testing is performed in San Francisco. The development team lead wants to ensure that the data stored in their test account Amazon S3 bucket is a current copy of the data in their production account Amazon S3 bucket. What steps implement the solution in the most effective way?

1. Configure S3 Bucket Lifecycle Policy.
2. Configure Cross-Region Replication.
3. Configure S3 Bucket Versioning.
4. Configure S3 Bucket Event Notification.
5. Configure an AWS Lambda function to replicate S3 objects.

EXPLANATION:

S3 Cross-Region Replication is S3 capability that can be configured on an S3 bucket to automatically replicate objects to another bucket in a different region. S3 bucket versioning is a requirement to enable S3 cross-region replication. S3 lifecycle policies are not related to replication of S3 data between accounts or regions. S3 lifecycle policies can be used to transition S3 objects to another Amazon S3 storage class (e.g. Glacier). Using S3 bucket event notifications for implementing object replication is not the optimal solution as it does not use S3 native capabilities. Implementing a Lambda function to replicate S3 objects to another bucket is not the optimal solution as it requires custom code development and testing.

Answer: b, c

You are an employee at a communications firm that is in the process of migrating its data to Amazon S3. The data will be stored in buckets and is sent to customers to do as they see fit. However, certain data is frequently changed when customers request revisions, while the rest of the data is rarely changed. You must be able to immediately access certain data while minimizing costs. Which S3 storage class should you choose?

1. S3 Intelligent Tiering
2. S3 Standard
3. S3 One Zone-Infrequent Access
4. S3 Glacier

EXPLANATION:

While S3 Glacier is a low-cost storage class, it is for data archiving and thus not ideal for frequent access or changes to data. And S3 One Zone-Infrequent Access is also low-cost, but it does not address the frequently changed data. Although S3 Standard is a suitable choice, since it addresses frequent access, it is not the least expensive choice for the less frequently accessed data. If it was hard to determine which data is frequently changed and which isn’t, S3 Standard might have been the most cost-effective choice. But in this case, S3 Intelligent Tiering is. Intelligent Tiering stores data in two access tiers: one tier is optimized for frequently accessed data while the other is a lower-cost tier for infrequent access.

Answer: a

Your company has been running its core application on a fleet of r4.xlarge EC2 instances for a year. You are confident that you understand the application steady-state performance and now you have been asked to purchase Reserved Instances (RIs) for a further 2 years to cover the existing EC2 instances, with the option of moving to other Memory or Compute optimised instance families when they are introduced. Which of the following options meet the above criteria whilst offering the greatest flexibility and maintaining the best value for money.

1. Purchase a 1 year Standard Zonal RI for 3 years, then sell the unused RI on the Reserved Instance Marketplace
2. Purchase a Convertible RI for 3 years, then sell the unused RI on the Reserved Instance Marketplace
3. Purchase a 1 year Convertible RI for each EC2 instance, for 2 consecutive years running
4. Purchase a Scheduled RI for 3 years, then sell the unused RI on the Reserved Instance Marketplace

EXPLANATION:

When answering this question, it's important to exclude those options which are not relevant, first. The question states that the RI should allow for moving between instance families and this immediately rules out Standard and Scheduled RIs as only Convertible RIs can do this. Of the 2 Convertible RI options, the first can be ruled out as it suggests selling unused RI capacity on the Reserved Instance Marketplace, but this is not available for Convertible RIs and therefore that only leaves one answer as being correct.

Answer: c

You have a static HTML website that requires inexpensive, highly available hosting solution that scales automatically to meet traffic demands. Which AWS service would best suit this requirement?

1. EC2 with EBS behind and Autoscaling Group with a minimum configuration of 2 instances
2. EC2 with EBS behind and Autoscaling Group with a minimum configuration of 1 instance
3. S3 - Static Website Hosting
4. EC2 with CloudFront

EXPLANATION:

S3 Static Website Hosting offers the best solution here: it is highly-available, scales automatically, and is cost-effective.

Answer: c

You have three AWS payer accounts consolidated under an AWS Organization . Which of the below statements is TRUE for purposes of volume discounts?

1. Usage in each account will be evaluated individually to determine the volume discount it is individually entitled to
2. Usage across the three accounts will be aggregated in determining the volume discount your Organization is entitled to
3. Usage across the three accounts will be aggregated in determining the volume discount your Organization is entitled to only if Consolidated Billing is enabled in each account
4. Usage across the three accounts will be aggregated in determining the volume discount your Organization is entitled to only if Consolidated Billing is enabled at the Organisation level

EXPLANATION:

If you have multiple accounts, your charges will decrease because AWS combines usage from all accounts in the organization to qualify you for volume pricing discounts.

Answer: b

You want to track the amount of money you ideally want your company to spend for EC2 data transfers every month. Which of the following actions will accomplish that?

1. Create a Reservation budget with AWS Budgets.
2. Create a Cost budget with AWS Budgets.
3. Enable AWS Cost Explorer
4. Create a Usage budget with AWS Budgets.

EXPLANATION:

AWS Cost Explorer is for providing information that you can use to track and manage costs, but it doesn’t enable the creation of budgets; that’s what AWS Budgets is for. If the question was strictly addressing cost, then creating a Cost budget with AWS Budgets would have been the correct answer. However, your concern is specifically with a usage type, which is EC2 data transfers. In this case, you would need to create a Usage budget with AWS Budgets and receive alerts when your defined threshold is met.

Answer: d