AWS Practise Paper- 5

Question 1:

You are designing an online banking application which needs to have a distributed session data management. Currently, the application is hosted on an Auto Scaling group of On-Demand EC2 instances across multiple Availability Zones with a Classic Load Balancer that distributes the load.

Which of the following options should you do to satisfy the given requirement?

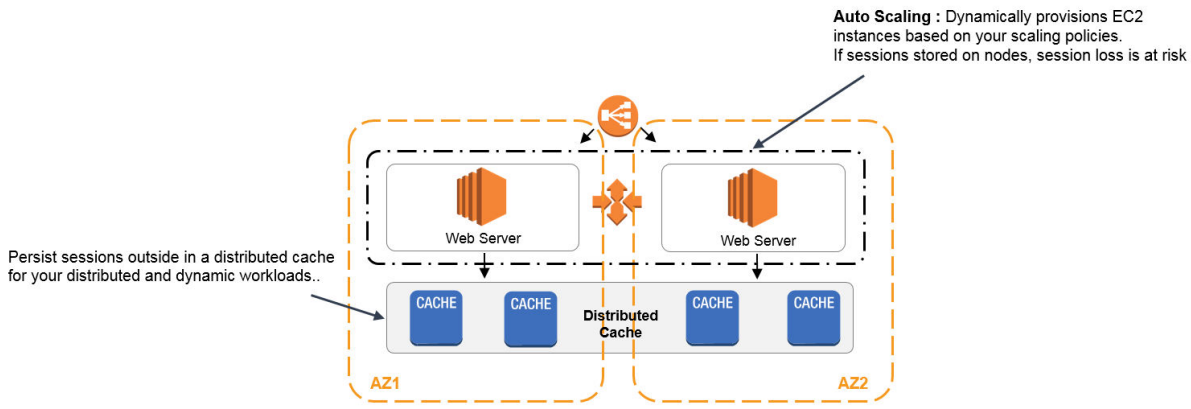
A. Set up an AWS Systems Manager Session Manager
B. Enable the sticky session feature in the Classic Load Balancer()
C. Use Amazon Elastic ache(Correct)
D. Use the GetSessionToken action in AWS STS for session management

EXPLANATION

In this question, the keyword is **distributed** session data management.

Sticky session feature of the Classic Load Balancer can also provide session management, however, take note that this feature has its limitations such as, in the event of a failure, you are likely to lose the sessions that were resident on the failed node. In the event that the number of your web servers change when your Auto Scaling kicks in, it's possible that the traffic may be unequally spread across the web servers as active sessions may exist on particular servers. If not mitigated properly, this can hinder the scalability of your applications. Hence, sticky session is not scalable or "**distributed**" as compared with ElastiCache.

You can manage HTTP session data from the web servers using an In-Memory Key/Value store such as Redis and Memcached. Redis is an open source, in-memory data structure store used as a database, cache, and message broker. Memcached is an in-memory key-value store for small arbitrary data (strings, objects) from results of database calls, API calls, or page rendering.



In AWS, you can use Amazon ElastiCache which offers fully managed Redis and Memcached service to manage and store session data for your web applications.

Option 1 is because the Session Manager is simply a capability that lets you manage your Amazon EC2 instances through an interactive one-click browser-based shell or through the AWS CLI. This does not act as a distributed session data management.

Option 2 is because although you can use the sticky session feature of the Classic Load Balancer to manage your session data, it is not a "distributed" solution compared to ElastiCache.

Option 4 is because the `GetSessionToken` is just one of the available actions in STS which returns a set of temporary credentials for an AWS account or IAM user. This is not used for distributed session data management.

Question 2:

A financial analytics application that collects, processes and analyses stock data in real-time is using Kinesis Data Streams. The producers continually push data to Kinesis Data Streams while the consumers process the data in real time. In Amazon Kinesis, where can the consumers store their results?

A. Amazon S3(Correct)
B. Glacier Select
C. Amazon Redshift(Correct)
D. AWS Glue
E. Amazon Athena

EXPLANATION:

In Amazon Kinesis, the producers continually push data to Kinesis Data Streams and the consumers process the data in real time. Consumers (such as a custom application running on Amazon EC2, or an Amazon Kinesis Data Firehose delivery stream) can store their results using an AWS service such as Amazon DynamoDB, Amazon Redshift, or Amazon S3.

Hence, Options 1 and 3 are the correct answers. The following diagram illustrates the high-level architecture of Kinesis Data Streams:

Option 2 is because Glacier Select is not a storage service. It is primarily used to run queries directly on data stored in Amazon Glacier, retrieving only the data you need out of your archives to use for analytics.

Option 4 is because AWS Glue is not a storage service. It is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics.

Option 5 is because Amazon Athena is just an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. It is not a storage service where you can store the results processed by the consumers.

Question 3:

An application which uses multiple EBS volumes could not cope with the growing storage requirements needed to store their data. Your IT Manager has instructed you to set up an S3 bucket as a replacement for their EBS volumes.

Which of the following options is correct regarding the naming convention for the S3 bucket?

A. **A bucket name must be unique across all existing bucket names in Amazon S3.(Correct)**
B. By default, an S3 bucket is not owned by the AWS account that created it()
C. Bucket names must be at least 5 and no more than 63 characters long.
D. Bucket names can be formatted as an IP address such as 192.168.5.4

EXPLANATION

The correct answer is: A bucket name must be unique across all existing bucket names in Amazon S3.

A bucket is owned by the AWS account that created it. By default, you can create up to 100 buckets in each of your AWS accounts. There is no limit to the number of objects that can be stored in a bucket and no difference in performance whether you use many buckets or just a few. You can store all of your objects in a single bucket, or you can organize them across several buckets.

The rules for DNS-compliant bucket names are as follows:

- -Bucket names must be at least 3 and no more than 63 characters long.
- -Bucket names must be a series of one or more labels. Adjacent labels are separated by a single period (.). Bucket names can contain lowercase letters, numbers, and hyphens. Each label must start and end with a lowercase letter or a number.
- -Bucket names must not be formatted as an IP address (for example, 192.168.5.4).
- -When using virtual hosted-style buckets with SSL, the SSL wildcard certificate only matches buckets that do not contain periods. To work around this, use HTTP or write your own certificate verification logic. We recommend that you do not use periods (".") in bucket names.

Question 4:

You are a Solutions Architect working for a major investment bank in London. Your IT Manager instructed you to prepare a migration plan from your on-premises application architecture to AWS. During your design process, you considered the current security of your on-premises application.

Which among the following does AWS provide for you as part of the shared responsibility model?

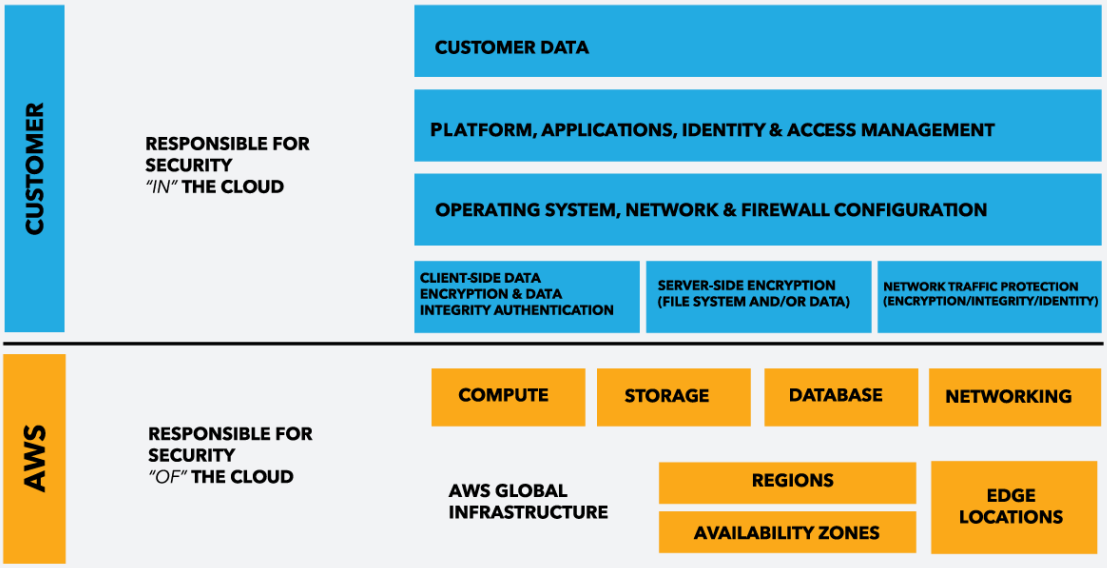
A. EC2 Instance security()
B. **Physical network infrastructure**(Correct)
C. User access to the AWS environment via IAM
D. Virtualization infrastructure(Correct)
E. Operating System (OS) patching for Spot and On-Demand EC2 instances

EXPLANATION

Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall.

Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment. As shown in the chart below, this differentiation of responsibility is commonly referred to as Security "of" the Cloud versus Security "in" the Cloud.

Refer to this diagram for a better understanding of the shared responsibility model.



Question 5:

You are setting up a configuration management in your existing cloud architecture where you have to deploy and manage your EC2 instances including the other AWS resources using Chef and Puppet. Which of the following is the most suitable service to use in this scenario?

A. **AWS OpsWorks(Correct)**
B. AWS Elastic Beanstalk
C. AWS CloudFormation()
D. AWS CodeDeploy

EXPLANATION

AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. Chef and Puppet are automation platforms that allow you to use code to automate the configurations of your servers. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed, and managed across your Amazon EC2 instances or on-premises compute environments.

Question 6:

You are working for a data analytics startup that collects clickstream data and stores them in an S3 bucket. You need to launch an AWS Lambda function to trigger your ETL jobs to run as soon as new data becomes available in Amazon S3.

Which of the following services can you use as an extract, transform, and load (ETL) service in this scenario?

A. S3 Select
B. Redshift Spectrum()
C. AWS Step Functions
D. AWS Glue(Correct)

EXPLANATION

AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. You can create and run an ETL job with a few clicks in the AWS Management Console. You simply point AWS Glue to your data stored on AWS, and AWS Glue discovers your data and stores the associated metadata (e.g. table definition and schema) in the AWS Glue Data Catalog. Once cataloged, your data is immediately searchable, queryable, and available for ETL. AWS Glue generates the code to execute your data transformations and data loading processes.

Question 7:
You are working as a solutions architect for a large financial company. They have a web application hosted in their on-premises infrastructure which they want to migrate to AWS cloud. Your manager had instructed you to ensure that there is no downtime while the migration process is on-going. In order to achieve this, your team had decided to divert 50% of the traffic to the new application in AWS and the other 50% to the application hosted in their on-premises infrastructure. Once the migration is over and the application works with no issues, a full diversion to AWS will be implemented.

Which of the following steps will you do to satisfy this requirement?

A. Use a Network Load balancer to divert the traffic between the on-premises and AWS-hosted application.()
B. Use an Application Elastic Load balancer to divert and proportion the traffic between the on-premises and AWS-hosted application.
C. Use Route 53 with Failover routing policy to divert and proportion the traffic between the on-premises and AWS-hosted application**.**

D. **Use Route 53 with Weighted routing policy to divert the traffic between the on-premises and AWS-hosted application.(Correct)**

EXPLANATION

To divert 50% of the traffic to the new application in AWS and the other 50% to the application, you can use Route53 with Weighted routing policy. This will divert the traffic between the on-premises and AWS-hosted application accordingly.

Weighted routing lets you associate multiple resources with a single domain name (tutorialsdojo.com) or subdomain name (learn.tutorialsdojo.com) and choose how much traffic is routed to each resource. This can be useful for a variety of purposes, including load balancing and testing new versions of software. You can set a specific percentage of how much traffic will be allocated to the resource by specifying the weights.

For example, if you want to send a tiny portion of your traffic to one resource and the rest to another resource, you might specify weights of 1 and 255. The resource with a weight of 1 gets 1/256th of the traffic (1/1+255), and the other resource gets 255/256ths (255/1+255).

You can gradually change the balance by changing the weights. If you want to stop sending traffic to a resource, you can change the weight for that record to 0.

Question 8:

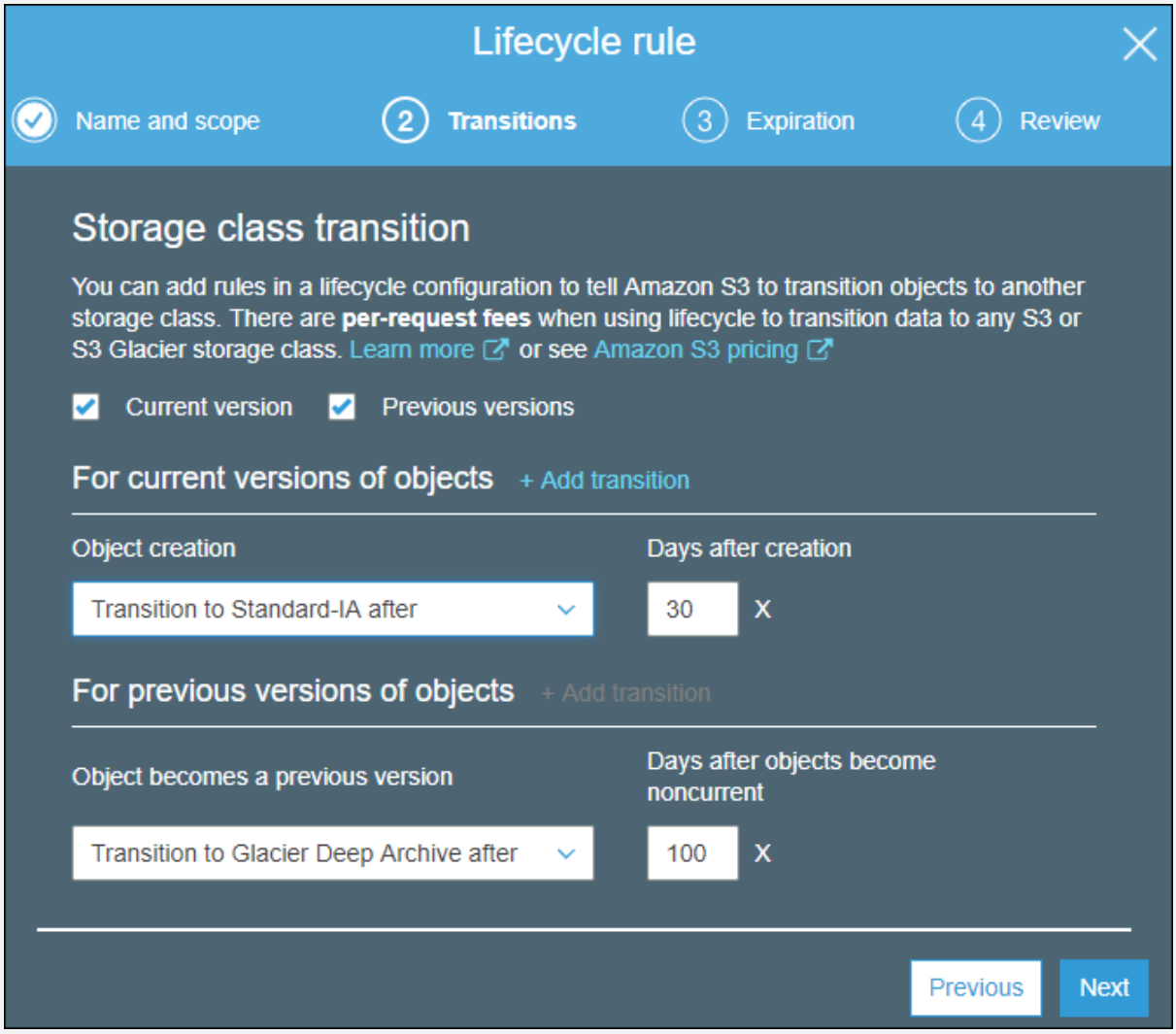
A company has 10 TB of infrequently accessed financial data that would need to be stored in AWS. These data would be accessed infrequently during specific weeks when they are retrieved for auditing purposes. The retrieval time is not strict as long as it does not exceed more than 24 hours.

Which of the following would be a secure, durable, and cost-effective solution for this scenario?

A. Upload the data to S3 then use a lifecycle policy to transfer data to S3-IA.
B. **Upload the data to S3 and set a lifecycle policy to transition data to Glacier after 0 days.(Correct)**
C. Upload the data directly to Amazon Glacier through the AWS Management Console.()
D. Upload the data to S3 then use a lifecycle policy to transfer data to S3 One Zone-IA.

EXPLANATION

Glacier is a cost-effective archival solution for large amounts of data. Bulk retrievals are S3 Glacier's lowest-cost retrieval option, enabling you to retrieve large amounts, even petabytes, of data inexpensively in a day. Bulk retrievals typically complete within 5 – 12 hours. You can specify an absolute or relative time period (including 0 days) after which the specified Amazon S3 objects should be transitioned to Amazon Glacier. Hence, Option 2 is the correct answer.



Option 1 is because using Glacier would be a more cost-effective solution than using S3-IA. Since required retrieval periods should not exceed more than a day, Glacier would be the best choice.

Option 3 is because you cannot upload objects to Amazon Glacier directly through the Management Console. To upload data, such as photos, videos, and other documents, you must either use the AWS CLI or write code to make requests, by using either the REST API directly or by using the AWS SDKs.

Option 4 is because with S3 One Zone-IA, the data will only be stored in a single availability zone and thus, this storage solution is not durable. It also costs more compared with Glacier, which is why this option is wrong.

Question 9:

You are building a prototype for a cryptocurrency news website of a small startup. The website will be deployed to a Spot EC2 instance and will use Amazon Aurora as its database. You requested a spot instance at a maximum

price of $0.04/hr which has been fulfilled immediately and after 90 minutes, the spot price increases to $0.06/hr and then your instance was terminated by AWS.

In this scenario, what would be the total cost of running your spot instance?

A. $0.08()
B. $0.07
C. $0.06(Correct)
D. $0.00
E. $0.04
F. $0.10

EXPLANATION

Since the Spot instance has been running for more than an hour, which is past the first instance hour, this means that you will be charged from the time it was launched till the time it was terminated by AWS. The computation for your 90 minute usage would be $0.04 (60 minutes) + $0.02 (30 minutes) = $0.06 hence, option 3 is correct.

If your Spot instance is terminated or stopped by Amazon EC2 in the first instance hour, you will not be charged for that usage. However, if you terminate the instance yourself, you will be charged to the nearest second.

If the Spot instance is terminated or stopped by Amazon EC2 in any subsequent hour, you will be charged for your usage to the nearest second. If you are running on Windows and you terminate the instance yourself, you will be charged for an entire hour.

Question 10:

You are working for a multinational telecommunications company. Your IT Manager is willing to consolidate their log streams including the access, application, and security logs in one single system. Once consolidated, the company wants to analyze these logs in real-time based on heuristics. There will be some time in the future where the company will need to validate heuristics, which requires going back to data samples extracted from the last 12 hours.

What is the best approach to meet this requirement?

A. First, set up an Auto Scaling group of EC2 servers then store the logs on Amazon S3 then finally, use EMR to apply heuristics on the logs.
B. First, send all of the log events to Amazon Kinesis then afterwards, develop a client process to apply heuristics on the logs.(Correct)
C. First, configure Amazon Cloud Trail to receive custom logs and then use EMR to apply heuristics on the logs.
D. First, send all the log events to Amazon SQS then set up an Auto Scaling group of EC2 servers to consume the logs and finally, apply the heuristics.

EXPLANATION
In this scenario, you need a service that can collect, process, and analyze data in real-time hence, the right service to use here is Amazon Kinesis.

Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information. Amazon Kinesis offers key capabilities to cost-effectively process streaming data at any scale, along with the flexibility to choose the tools that best suit the requirements of your application.
With Amazon Kinesis, you can ingest real-time data such as video, audio, application logs, website clickstreams, and IoT telemetry data for machine learning, analytics, and other applications. Amazon Kinesis enables you to process and analyze data as it arrives and respond instantly instead of having to wait until all your data is collected before the processing can begin.

Question 11:

A leading e-commerce company is in need of a storage solution that can be accessed by 1000 Linux servers in multiple availability zones. The service should be able to handle the rapidly changing data at scale while still maintaining high performance. It should also be highly durable and highly available whenever the servers will pull data from it, with little need for management.

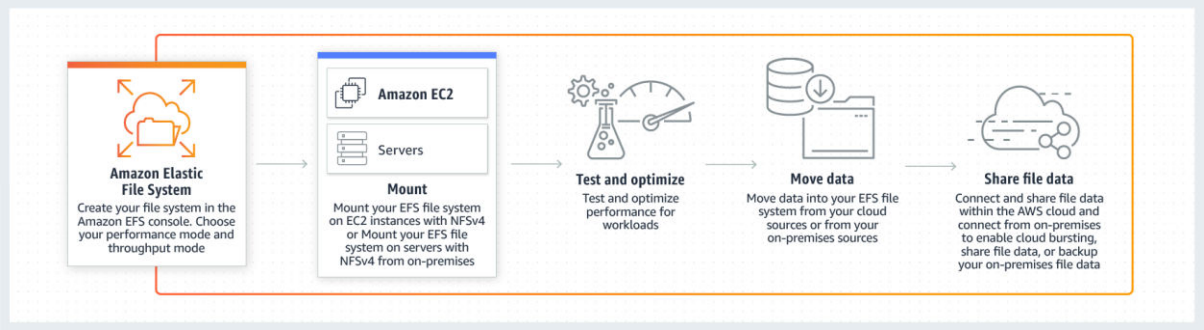
As the Solutions Architect, which of the following services is the most cost-effective choice that you should use to meet the above requirement?

A. S3
B. EFS(Correct)
C. EBS()
D. Storage Gateway

EXPLANATION

Amazon Web Services (AWS) offers cloud storage services to support a wide range of storage workloads such as EFS, S3 and EBS. You have to understand when you should use Amazon EFS, Amazon S3 and Amazon Elastic Block Store (EBS) based on the specific workloads. In this scenario, the keywords are ***rapidly changing data*** and 1000 Linux servers.

Amazon EFS is a file storage service for use with Amazon EC2. Amazon EFS provides a file system interface, file system access semantics (such as strong consistency and file locking), and concurrently-accessible storage for **up to thousands of Amazon EC2 instances**. EFS provides the same level of high availability and high scalability like S3 however, this service is more suitable for scenarios where it is required to have a POSIX-compatible file system or if you are storing rapidly changing data.



Data that must be updated very frequently might be better served by storage solutions that take into account read and write latencies, such as Amazon EBS volumes, Amazon RDS, Amazon DynamoDB, Amazon EFS, or relational databases running on Amazon EC2.

Amazon EBS is a block-level storage service for use with Amazon EC2. Amazon EBS can deliver performance for workloads that require the lowest-latency access to data from a single EC2 instance.

Amazon S3 is an object storage service. Amazon S3 makes data available through an Internet API that can be accessed anywhere.

In this scenario, Option 2 is the best answer. As stated above, Amazon EFS provides a file system interface, file system access semantics (such as strong consistency and file locking), and concurrently-accessible storage for **up to thousands of Amazon EC2 instances**. EFS provides the performance, durability, high availability, and storage capacity needed by the 1000 Linux servers in the scenario.

Option 1 is because although S3 provides the same level of high availability and high scalability like EFS, this service is not suitable for storing data which are rapidly changing, just as mentioned in the above EXPLANATION. It is still more effective to use EFS as it offers strong consistency and file locking which the S3 service lacks.

Option 3 is because an EBS Volume cannot be shared by multiple instances.

Option 4 is because Storage Gateway is primarily used to extend the storage of your on-premises data center to your AWS Cloud.

Question 12:

A Junior DevOps Engineer deployed a large EBS-backed EC2 instance to host a NodeJS web app in AWS which was developed by an IT contractor. He properly configured the security group and used a key pair named "tutorialsdojokey" which has a tutorialsdojokey.pem private key file. The EC2 instance works as expected and the junior DevOps engineer can connect to it using an SSH connection. The IT contractor was also given the key pair and he has made various changes in the instance as well to the files located in .ssh folder to make the NodeJS app work. After a few weeks, the IT contractor and the junior DevOps engineer cannot connect the EC2 instance anymore, even with a valid private key file. They are constantly getting a "Server refused our key" error even though their private key is valid.

In this scenario, which one of the following options is not a possible reason for this issue?

A. You're using an SSH private key but the corresponding public key is not in the authorized_keys file.()
B. You don't have permissions for your authorized_keys file.
C. You don't have permissions for the .ssh folder.
D. The SSH private key that you are using has a file permission of 0777.(Correct)

EXPLANATION

All of the options here are correct except for Option 4 because if the private key that you are using has a file permission of 0777, then it will throw an "Unprotected Private Key File" error and not a "Server refused our key" error.

You might be unable to log into an EC2 instance if:

- You're using an SSH private key but the corresponding public key is not in the authorized_keys file.
- You don't have permissions for your authorized_keys file.
- You don't have permissions for the .ssh folder.
- Your authorized_keys file or .ssh folder isn't named correctly.
- Your authorized_keys file or .ssh folder was deleted.
- Your instance was launched without a key, or it was launched with an key.

To connect to your EC2 instance after receiving the error "Server refused our key," you can update the instance's user data to append the specified SSH public key to the authorized_keys file, which sets the appropriate ownership and file permissions for the SSH directory and files contained in it.

Question 13:

You are implementing a hybrid architecture for your company where you are connecting their Amazon Virtual Private Cloud (VPC) to their on-premises network. Which of the following can be used to create a private connection between the VPC and your company's on-premises network?

A. Direct Connect(Correct)
B. Route 53
C. ClassicLink()
D. AWS Direct Link

EXPLANATION

Direct Connect creates a direct, private connection from your on-premises data center to AWS, letting you establish a 1-gigabit or 10-gigabit dedicated network connection using Ethernet fiber-optic cable.

Question 14:

Your IT Director instructed you to ensure that all of the AWS resources in your VPC don't go beyond their service limit.

Which of the following services can help in this task?

A. AWS Cloudwatch
B. AWS EC2()
C. AWS Trusted Advisor(Correct)
D. AWS SNS

EXPLANATION

Remember that the AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in these five categories: Cost Optimization, Performance, Fault Tolerance, Security, and Service Limits. You can use a mnemonic, such as CPFSS, to memorize these five categories.

Question 15:

An online shopping platform is hosted on an Auto Scaling group of On-Demand EC2 instances with a default Auto Scaling termination policy and no instance protection configured. The system is deployed across three Availability Zones in the US West region (us-west-1) with an Application Load Balancer in front to provide high availability and fault tolerance for the shopping platform. The us-west-1a, us-west-1b, and us-west-1c Availability Zones have 10, 8 and 7 running instances respectively. Due to the low number of incoming traffic, the scale-in operation has been triggered.

Which of the following will the Auto Scaling group do to determine which instance to terminate first in this scenario?

Choose the Availability Zone with the most number of instances, which is the us-west-1a Availability Zone in this scenario.(Correct)

A. Choose the Availability Zone with the least number of instances, which is the us-west-1c Availability Zone in this scenario.
B. Select the instances with the most recent launch configuration.
C. Select the instances with the oldest launch configuration.(Correct)
D. Select the instance that is closest to the next billing hour.(Correct)
E. Select the instance that is farthest to the next billing hour.

EXPLANATION

The default termination policy is designed to help ensure that your network architecture spans Availability Zones evenly. With the default termination policy, the behavior of the Auto Scaling group is as follows:

1. If there are instances in multiple Availability Zones, choose the Availability Zone with the most instances and at least one instance that is not protected from scale in.

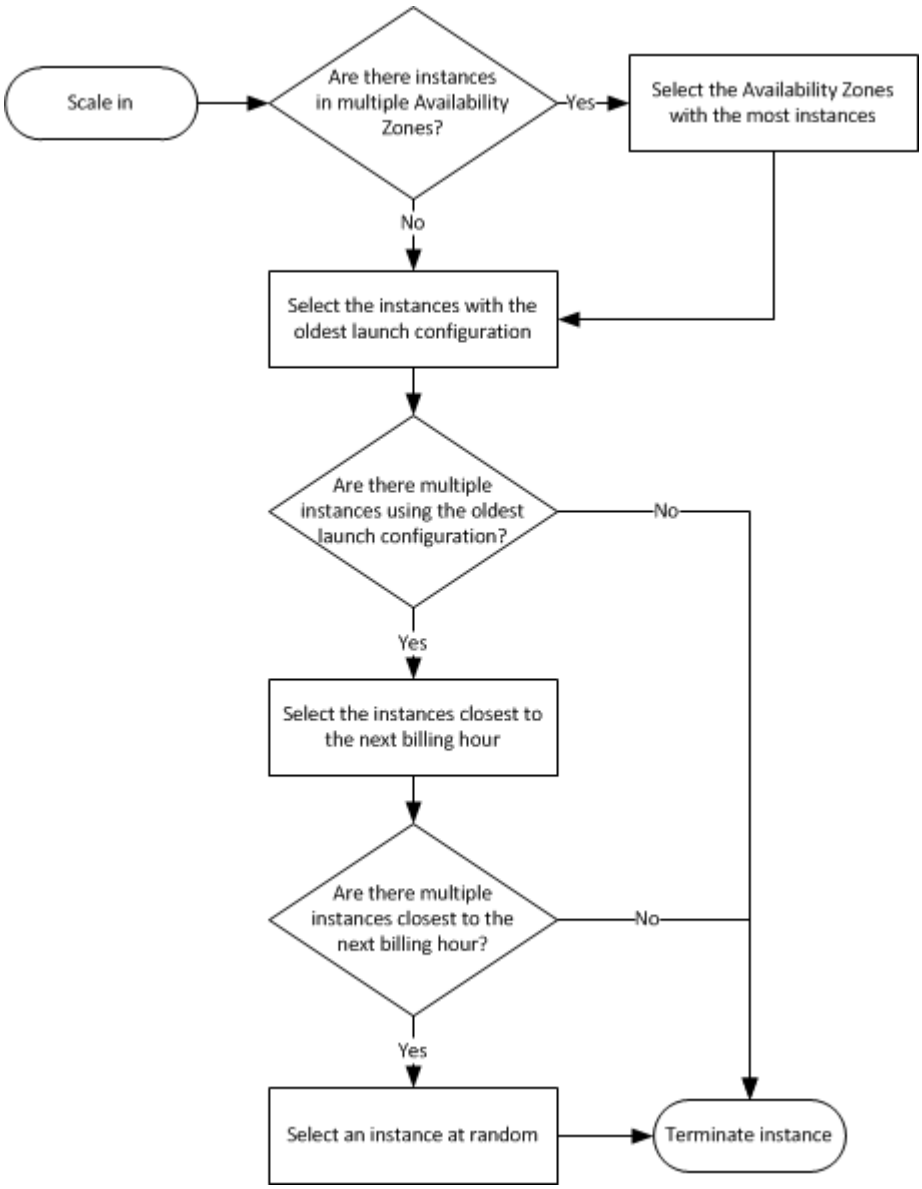
If there is more than one Availability Zone with this number of instances, choose the Availability Zone with the instances that use the oldest launch configuration.

2. Determine which unprotected instances in the selected Availability Zone use the oldest launch configuration. If there is one such instance, terminate it.

3. If there are multiple instances to terminate based on the above criteria, determine which unprotected instances are closest to the next billing hour. (This helps you maximize the use of your EC2 instances and manage your Amazon EC2 usage costs.) If there is one such instance, terminate it.

4. If there is more than one unprotected instance closest to the next billing hour, choose one of these instances at random.

The following flow diagram illustrates how the default termination policy works:



Question 16:

You are tasked to choose the most affordable AWS support plan that offers the following:

1.) 24x7 access to customer service, documentation, whitepapers, and support forums.

2.) Access to full set of Trusted Advisor checks

Which type of support plan will you choose?

A. Basic
B. Developer()
C. Business(Correct)
D. Enterprise

EXPLANATION

There are 4 types of AWS support plans:

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

All customers receive Basic Support included with your AWS account. All plans, including Basic Support, provide 24x7 access to customer service, AWS documentation, whitepapers, and support forums.

Business and Enterprise plans provide access to full set of Trusted Advisor checks. However, the main question here which is the most affordable. Hence, the best answer is the Business plan since it is cheaper than the Enterprise plan.

Question 17:

You are planning to migrate an enterprise application from your on-premises network to AWS cloud. You are looking for managed services in AWS that automatically takes care of the maintenance of the underlying resources such as OS patching and security management.

Which AWS services should you use to migrate the application? (Choose 2)

A. Elastic Beanstalk
B. RDS(Correct)
C. DynamoDB(Correct)
D. Amazon EC2 Dedicated Hosts
E. Amazon Redshift Spectrum
F. Amazon Elastic MapReduce

EXPLANATION

The keyword in the question is managed service. This means that AWS will manage the underlying resources for the service. Amazon RDS and DynamoDB are examples of managed services in AWS.

Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. It is a fully managed cloud database and supports both document and key-value store models.

Amazon Relational Database Service (Amazon RDS) is a managed service that makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while managing time-consuming database administration tasks, enabling you to focus on your applications and business.

Options 1 and 6 are because both Elastic Beanstalk and Amazon Elastic MapReduce automatically provision EC2 instances which you still need to manage yourself. Hence, these are not managed services that you can use for this scenario.

Option 4 is because you will still need to manage Amazon EC2 Dedicated Hosts. Take note that EC2 instances are not managed services which means that you are responsible for maintaining the health of the instance and applying the required OS patches.

Option 5 is because Amazon Redshift Spectrum is primarily used to query open file formats in Amazon S3 and data in Redshift in a single query, without the need or delay of loading the S3 data. Although Redshift is a fully-managed service, take note that Amazon Redshift Spectrum is simply a tool and is not applicable in this scenario.

Question 18:

An application is hosted on an EC2 instance with multiple EBS Volumes attached and uses Amazon Neptune as its database. To improve data security, you encrypted all of the EBS volumes attached to the instance to protect the confidential data stored in the volumes.

Which of the following statements are true about encrypted Amazon Elastic Block Store volumes?

•

A. **All data moving between the volume and the instance are encrypted. (Correct)**
B. **Snapshots are automatically encrypted. (Correct)**
C. Snapshots are not automatically encrypted.
D. Existing volumes can be encrypted.
E. Shared volumes can be encrypted.

EXPLANATION

Amazon Elastic Block Store (Amazon EBS) provides block level storage volumes for use with EC2 instances. EBS volumes are highly available and reliable storage volumes that can be attached to any running instance that is in the same Availability Zone. EBS volumes that are attached to an EC2 instance are exposed as storage volumes that persist independently from the life of the instance.

When you create an encrypted EBS volume and attach it to a supported instance type, the following types of data are encrypted:

- Data at rest inside the volume
- All data moving between the volume and the instance
- All snapshots created from the volume
- All volumes created from those snapshots

There is no direct way to encrypt an existing unencrypted volume or to remove encryption from an encrypted volume. However, you can migrate data between encrypted and unencrypted volumes.

Question 19:

You have EC2 instances running on your VPC. You have both UAT and production EC2 instances running. You want to ensure that employees who are responsible for the UAT instances don't have the access to work on the production instances to minimize security risks.

Which of the following would be the best way to achieve this?

A. Launch the UAT and production EC2 instances in separate VPC's connected by VPC peering.()
B. Create an IAM policy with a condition which allows access to only EC2 instances that are used for production or development.
C. Launch the UAT and production instances in different Availability Zones and use Multi Factor Authentication.
D. Define the tags on the UAT and production servers and add a condition to the IAM policy which allows access to specific tags.(Correct)

EXPLANATION

For this scenario, the best way to achieve this solution is to use a combination of Tags and IAM policies. You can define the tags on the UAT and production EC2 instances and add a condition to the IAM policy which allows access to specific tags.

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it.

By default, IAM users don't have permission to create or modify Amazon EC2 resources, or perform tasks using the Amazon EC2 API. (This means that they also can't do so using the Amazon EC2 console or CLI.) To allow IAM users to create or modify resources and perform tasks, you must create IAM policies that grant IAM users permission to use the specific resources and API actions they'll need, and then attach those policies to the IAM users or groups that require those permissions.

Question 20:

You are working for a top IT Consultancy and one of your clients asked you how to properly secure their AWS infrastructure. They have a VPC with two On-Demand EC2 instances with Elastic IP addresses which recently were under SSH brute force attacks over the Internet. Their IT Security team has identified the IP addresses where these attacks originated.

Which of the following is the quickest way to fix this security vulnerability?

A. Place the EC2 instances into private subnets()
B. Remove the Internet Gateway from the VPC
C. Block the IP addresses in the Network Access Control List(Correct)
D. Deploy the EC2 instances into private subnets then set up a bastion host

EXPLANATION

A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

The following are the basic things that you need to know about network ACLs:

- Your VPC automatically comes with a modifiable default network ACL. By default, it allows all inbound and outbound IPv4 traffic and, if applicable, IPv6 traffic.

- You can create a custom network ACL and associate it with a subnet. By default, each custom network ACL denies all inbound and outbound traffic until you add rules.

- Each subnet in your VPC must be associated with a network ACL. If you don't explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL.

- You can associate a network ACL with multiple subnets; however, a subnet can be associated with only one network ACL at a time. When you associate a network ACL with a subnet, the previous association is removed.

- A network ACL contains a numbered list of rules that we evaluate in order, starting with the lowest numbered rule, to determine whether traffic is allowed in or out of any subnet associated with the network ACL. The highest number that you can use for a rule is 32766. We recommend that you start by creating rules in increments (for example, increments of 10 or 100) so that you can insert new rules where you need to later on.

- A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic.

- Network ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa).

The scenario clearly states that it requires the quickest way to fix the security vulnerability. In this situation, you can manually block the offending IP addresses

using Network ACLs since the IT Security team already identified the list of offending IP addresses. Alternatively, you can set up a bastion host however, this option entails additional time to properly set up as you have to configure the security configurations of your bastion host. Hence, Option 3 is the best answer since it can quickly resolve the issue by blocking the IP addresses using Network ACL.

Option 1 is because if you deploy the EC2 instance in the private subnet without public or EIP address, it would not be accessible over the Internet, even to you.

Option 2 is because removing the Internet Gateway will also make your EC2 instance inaccessible to you as it will cut down the connection to the Internet.

Option 4 is a valid answer, however, setting up a bastion host is not the quickest way to fix the security vulnerability as opposed to using Network ACLs. This entails additional time to properly set up and, in addition, you still have to worry about doing the proper Security Group and NACL configurations of your bastion host. Moreover, the scenario explicitly says that the IT Security team have already identified the list of offending IP addresses. Remember that you primarily use Network ACL if you want to block an IP address on the subnet level. If you used a bastion host, then you will also need to use a Network ACL to block those offending IP addresses in the first place. Hence, this option is .

Question 21:

You are assigned to design a highly available architecture in AWS. You have two target groups with three EC2 instances each, which are added to an Application Load Balancer. In the security group of the EC2 instance, you have verified that the port 80 for HTTP is allowed. However, the instances are still showing out of service.

A. What could be the root cause of this issue?
B. The instances are using the wrong AMI.()
C. The health check configuration is not properly defined.(Correct)
D. The wrong instance type was used for the EC2 instance.
E. The wrong subnet was used in your VPC

EXPLANATION

Since the security group is properly configured, the issue may be caused by a wrong health check configuration in the Target Group.

Your Application Load Balancer periodically sends requests to its registered targets to test their status. These tests are called health checks. Each load balancer node routes requests only to the healthy targets in the enabled Availability Zones for the load balancer. Each load balancer node checks the health of each target, using the health check settings for the target group with which the target is registered. After your target is registered, it must pass one health check to be considered healthy. After each health check is completed, the load balancer node closes the connection that was established for the health check.

Question 22:

You have an existing On-demand EC2 instance and you are planning to create a new EBS volume that will be attached to this instance. The data that will be stored are confidential medical records so you have to make sure that the data is protected. How can you secure the data at rest of the new EBS volume that you will create?

A. Encrypt the EBS volume using the S3 server-side encryption service.()
B. Encrypt the EBS volume using the S3 client-side encryption service.
C. Create the EBS Volume first and attach it to the instance then enable encryption.
D. In IAM, create a new policy that disallows any read and write access to the EBS volume.
E. Create an encrypted EBS Volume by ticking the encryption tickbox and attach it to the instance. (Correct)

EXPLANATION

You can secure the data at rest by creating an encrypted EBS Volume. The main difference between creating an unencrypted to an encrypted EBS Volume is just one tickbox called "Encryption". You can create an encrypted EBS Volume by ticking the encryption tickbox and attach it to the EC2 instance.

Amazon EBS encryption offers a simple encryption solution for your EBS volumes without the need to build, maintain, and secure your own key management infrastructure. When you create an encrypted EBS volume and attach it to a supported instance type, the following types of data are encrypted:

- -Data at rest inside the volume
- -All data moving between the volume and the instance
- -All snapshots created from the volume
- -All volumes created from those snapshots

Encryption operations occur on the servers that host EC2 instances, ensuring the security of both data-at-rest and data-in-transit between an instance and its attached EBS storage.

Options 1 and 2 are since you can't use the server and client-side encryption of S3 in EBS Volumes.

Option 3 is due to the fact that there is no direct way to encrypt an already existing unencrypted volume that you have created. You can only do it by enabling encryption during the time when you created the EBS Volume.

Option 4 is because you cannot encrypt an EBS Volume using IAM.

Question 23:

You are managing a global news website which has a very high traffic. To improve the performance, you redesigned the application architecture to use a Classic Load Balancer with an Auto Scaling Group in multiple Availability

Zones. However, you noticed that one of the Availability Zones is not receiving any traffic. What is the root cause of this issue?

A. Auto Scaling should be disabled for the load balancer to route the traffic to multiple Availability Zones.
B. By default, you are not allowed to use a load balancer with multiple Availability Zones. You have to send a request form to AWS in order for this to work.()
C. The Availability Zone is not properly added to the load balancer which is why it is not receiving any traffic. (Correct)
D. The Classic Load Balancer is down

EXPLANATION

In this scenario, one of the Availability Zones is not properly added to the Elastic load balancer. Hence, that Availability Zone is not receiving any traffic.

You can set up your load balancer in EC2-Classic to distribute incoming requests across EC2 instances in a single Availability Zone or multiple Availability Zones. First, launch EC2 instances in all the Availability Zones that you plan to use. Next, register these instances with your load balancer. Finally, add the Availability Zones to your load balancer. After you add an Availability Zone, the load balancer starts routing requests to the registered instances in that Availability Zone. Note that you can modify the Availability Zones for your load balancer at any time.

By default, the load balancer routes requests evenly across its Availability Zones. To route requests evenly across the registered instances in the Availability Zones, enable cross-zone load balancing.

Question 24:

A leading media company has recently adopted a hybrid cloud architecture which requires them to migrate their application servers and databases in AWS. One of their applications requires a heterogeneous database migration in which you need to transform your on-premises Oracle database to PostgreSQL in AWS. This entails a schema and code transformation before the proper data migration starts.

Which of the following options is the most suitable approach to migrate the database in AWS?

A. Configure a Launch Template that automatically converts the source schema and code to match that of the target database. Then, use the AWS Database Migration Service to migrate data from the source database to the target database. ()
B. **First, use the AWS Schema Conversion Tool to convert the source schema and code to match that of the target database, and then use the AWS Database Migration Service to migrate data from the source database to the target database. (Correc**t)
C. Use Amazon Neptune to convert the source schema and code to match that of the target database in RDS. Use the AWS Batch to effectively migrate the data from the source database to the target database in a batch process.

D. Heterogeneous database migration is not supported in AWS. You have to transform your database first to PostgreSQL and then migrate it to RDS.

EXPLANATION

AWS Database Migration Service helps you migrate databases to AWS quickly and securely. The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database. The AWS Database Migration Service can migrate your data to and from most widely used commercial and open-source databases.

AWS Database Migration Service can migrate your data to and from most of the widely used commercial and open source databases. It supports homogeneous migrations such as Oracle to Oracle, as well as heterogeneous migrations between different database platforms, such as Oracle to Amazon Aurora. Migrations can be from on-premises databases to Amazon RDS or Amazon EC2, databases running on EC2 to RDS, or vice versa, as well as from one RDS database to another RDS database. It can also move data between SQL, NoSQL, and text based targets.

In heterogeneous database migrations the source and target databases engines are different, like in the case of Oracle to Amazon Aurora, Oracle to PostgreSQL, or Microsoft SQL Server to MySQL migrations. In this case, the schema structure, data types, and database code of source and target databases can be quite different, requiring a schema and code transformation before the data migration starts. That makes heterogeneous migrations a two step process. First use the AWS Schema Conversion Tool to convert the source schema and code to match that of the target database, and then use the AWS Database Migration Service to migrate data from the source database to the target database. All the required data type conversions will automatically be done by the AWS Database Migration Service during the migration. The source database can be located in your own premises outside of AWS, running on an Amazon EC2 instance, or it can be an Amazon RDS database. The target can be a database in Amazon EC2 or Amazon RDS.

Option 1 is because Launch templates are primarily used in EC2 to enable you to store launch parameters so that you do not have to specify them every time you launch an instance.

Option 3 is because Amazon Neptune is a fully-managed graph database service and not a suitable service to use to convert the source schema. AWS Batch is not a database migration service and hence, it is not suitable to be used in this scenario. You should use the AWS Schema Conversion Tool and AWS Database Migration Service instead.

Option 4 is because heterogeneous database migration is supported in AWS using the Database Migration Service.

Question 25:

You recently launched a fleet of on-demand EC2 instances to host a massively multiplayer online role-playing game (MMORPG) server in your VPC. The EC2 instances are configured with Auto Scaling and AWS Systems Manager. What

can you use to configure your EC2 instances without having to establish a RDP or SSH connection to each instance?

A. AWS Config
B. AWS CodePipeline()
C. Run Command(Correct)
D. EC2Config

EXPLANATION

You can use Run Command from the console to configure instances without having to login to each instance.

AWS Systems Manager Run Command lets you remotely and securely manage the configuration of your managed instances. A managed instance is any Amazon EC2 instance or on-premises machine in your hybrid environment that has been configured for Systems Manager. Run Command enables you to automate common administrative tasks and perform ad hoc configuration changes at scale. You can use Run Command from the AWS console, the AWS Command Line Interface, AWS Tools for Windows PowerShell, or the AWS SDKs. Run Command is offered at no additional cost.

Question 26:

A Dedicated EC2 instance retrieves a message from an SQS queue and begins processing the message. After five minutes, the instance crashes.

What happens to the message?

A. When the message visibility timeout expires, the message becomes available for processing by other EC2 instances(Correct)
B. It will remain in the queue and still assigned to same EC2 instances when instances become online within the visibility timeout.()
C. The message is deleted and becomes duplicated in the SQS when the EC2 instance comes online.

EXPLANATION

When a consumer receives and processes a message from a queue, the message remains in the queue. Amazon SQS doesn't automatically delete the message. Because Amazon SQS is a distributed system, there's no guarantee that the consumer actually receives the message (for example, due to a connectivity issue, or due to an issue in the consumer application). Thus, the consumer must delete the message from the queue after receiving and processing it.

Immediately after the message is received, it remains in the queue. To prevent other consumers from processing the message again, Amazon SQS sets a visibility timeout, a period of time during which Amazon SQS prevents other consumers from receiving and processing the message. The default visibility timeout for a message is 30 seconds. The maximum is 12 hours.

Question 27:

You are an IT Consultant for a top investment bank which is in the process of building its new Forex trading platform. To ensure high availability and scalability, you designed the trading platform to use an Elastic Load Balancer in front of an Auto Scaling group of On-Demand EC2 instances across multiple Availability Zones. For its database tier, you chose to use a single Amazon Aurora instance to take advantage of its distributed, fault-tolerant and self-healing storage system.

In the event of system failure on the primary database instance, what happens to Amazon Aurora during the failover?

A. Amazon Aurora flips the canonical name record (CNAME) for your DB Instance to point at the healthy replica, which in turn is promoted to become the new primary.()
B. **Aurora will first attempt to create a new DB Instance in the same Availability Zone as the original instance. If unable to do so, Aurora will attempt to create a new DB Instance in a different Availability Zone.(Correct**)
C. Amazon Aurora flips the A record of your DB Instance to point at the healthy replica, which in turn is promoted to become the new primary.
D. Aurora will first attempt to create a new DB Instance in a different Availability Zone of the original instance. If unable to do so, Aurora will attempt to create a new DB Instance in the original Availability Zone in which the instance was first launched.

EXPLANATION

Failover is automatically handled by Amazon Aurora so that your applications can resume database operations as quickly as possible without manual administrative intervention.

If you have an Amazon Aurora Replica in the same or a different Availability Zone, when failing over, Amazon Aurora flips the canonical name record (CNAME) for your DB Instance to point at the healthy replica, which in turn is promoted to become the new primary. Start-to-finish, failover typically completes within 30 seconds.

If you do not have an Amazon Aurora Replica (i.e. single instance), Aurora will first attempt to create a new DB Instance in the same Availability Zone as the original instance. If unable to do so, Aurora will attempt to create a new DB Instance in a different Availability Zone. From start to finish, failover typically completes in under 15 minutes.

Hence, the correct answer is Option 2.

Options 1 and 3 are because this will only happen if you are using an Amazon Aurora Replica. In addition, Amazon Aurora flips the canonical name record (CNAME) and not the A record (IP address) of the instance.

Option 4 is because Aurora will first attempt to create a new DB Instance in the same Availability Zone as the original instance. If unable to do so, Aurora will attempt to create a new DB Instance in a different Availability Zone and not the other way around.

Question 28:

You have a web application hosted on a fleet of EC2 instances located in two Availability Zones that are all placed behind an Application Load Balancer. As a Solutions Architect, you have to add a health check configuration to ensure your application is highly-available.

Which health checks will you implement?

- **A. HTTP or HTTPS health check(Correct)**
- B. ICMP health check
- C. FTP health check()
- D. TCP health check

EXPLANATION

The type of ELB that is mentioned here is an Application Elastic Load Balancer. This is used if you want a flexible feature set for your web applications with HTTP and HTTPS traffic. Conversely, it only allows 2 types of health check: HTTP and HTTPS.

Options 2 and 3 are as FTP and ICMP health checks are not supported.

Option 4 is . A TCP health check is only offered in Network Load Balancer, which is another type of ELB. It is used if you need ultra-high performance and static IP addresses for your application.

Question 29:

In a startup company you are working for, you are asked to design a web application that requires a NoSQL database that has no limit on the request capacity or storage size for a given table. The startup is still new in the market and it has very limited human resources who can take care of the database infrastructure.

Which is the most suitable service that you can implement that provides a fully managed, scalable and highly available NoSQL service?

- **A. DynamoDB(Correct)**
- B. Amazon Neptune
- C. Amazon Aurora
- D. SimpleDB

EXPLANATION

The term "fully managed" means that Amazon will manage the underlying infrastructure of the service hence, you don't need an additional human resource to support or maintain the service. Therefore, Amazon DynamoDB is the right answer. Remember that Amazon RDS is a managed service but not "fully managed" as you still have the option to maintain and configure the underlying server of the database.

Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. It is a fully managed cloud database and supports both document and key-value store models. Its flexible data model, reliable performance, and automatic scaling of

throughput capacity make it a great fit for mobile, web, gaming, ad tech, IoT, and many other applications.

Option 2 is because Amazon Neptune is primarily used as a graph database.

Option 3 is because Amazon Aurora is a relational database and not a NoSQL database.

Option 4 is because although SimpleDB is also a highly available and scalable NoSQL database, it has a limit on the request capacity or storage size for a given table, unlike DynamoDB.

Question 30:

A web application is deployed in an On-Demand EC2 instance in your VPC. There is an issue with the application which requires you to connect to it via an SSH connection. Which of the following is needed in order to access an EC2 instance from the Internet?

A. **An Internet Gateway (IGW) attached to the VPC.(Correc**t)
B. A Private IP address attached to the EC2 instance.
C. A Private Elastic IP address attached to the EC2 instance.()
D. A VPN Peering connection.
E. **A route entry to the Internet gateway in the Route table of the VPC.(Correct)**
F. **A Public IP address attached to the EC2 instance.(Correct)**

EXPLANATION

Options 1, 5, and 6 are the correct answers. In order for you to access your EC2 instance from the Internet, you need to have:

1. An Internet Gateway (IGW) attached to the VPC.
2. A route entry to the Internet gateway in the Route table of the VPC.
3. A Public IP address attached to the EC2 instance.

Option 2 is as you only use a Private IP inside your VPC.

Option 3 is as an Elastic IP Address is a public IPv4 address, not private. It is reachable from the Internet and is designed for dynamic cloud computing.

Option 4 is as you only use VPC Peering to connect two VPCs.

Question 31:

A news company has been using a Hardware Security Module (CloudHSM) for secure key storage. It is only used for generating keys for their On-demand EC2 instances. After a new support staff attempted to log in as the administrator three times using an invalid password, the Hardware Security Module has been zeroized which means that the encryption keys on it have

been wiped. Unfortunately, you did not have a copy of the keys stored anywhere else.

How can you obtain a new copy of the keys that you have stored on Hardware Security Module?

A. Restore a snapshot of the Hardware Security Module.()
B. Contact AWS Support and they will provide you a copy of the keys.
C. The keys are lost permanently if you did not have a copy.(Correct)
D. Use the Amazon CLI to get a copy of the keys.

EXPLANATION

Intentionally enter an administrator password three times in a row. Attempting to log in as the administrator more than twice with the wrong password zeroizes your HSM appliance. When an HSM is zeroized, all keys, certificates, and other data on the HSM is destroyed. You can use your cluster's security group to prevent an unauthenticated user from zeroizing your HSM.

Amazon does not have access to your keys nor credentials of your Hardware Security Module (HSM) and therefore has no way to recover your keys if you lose your credentials. Amazon strongly recommends that you use two or more HSMs in separate Availability Zones in any production CloudHSM Cluster to avoid loss of cryptographic keys.

Question 32:

You created a new CloudFormation template that creates 4 EC2 instances and are connected to one Elastic Load Balancer (ELB). Which section of the template should you configure to get the Domain Name Server hostname of the ELB upon the creation of the AWS stack?

A. Resources
B. Parameters()
C. Outputs(Correct)
D. Mappings

EXPLANATION

Outputs is an optional section of the CloudFormation template that describes the values that are returned whenever you view your stack's properties.

Question 33:

You are working as an IT Consultant for a large financial firm. They have a requirement to store irreproducible financial documents using Amazon S3. For their quarterly reporting, the files are required to be retrieved after a period of 3 months. There will be some occasions when a surprise audit will be held, which requires access to the archived data that they need to present immediately.

What will you do to satisfy this requirement in a cost-effective way?

A. Use Amazon S3 Standard()
B. Use Amazon S3 Standard - Infrequent Access(Correct)
C. Use Amazon S3 -Intelligent Tiering

D. Use Amazon Glacier

EXPLANATION

In this scenario, the requirement is to have a storage option that is cost-effective and has the ability to access or retrieve the archived data within an hour. The cost-effective options are Amazon Glacier and Amazon S3 Standard- Infrequent Access (Standard - IA). However, the former option is not designed for rapid retrieval of data which is required for the surprise audit. Hence, option 4 is wrong and the best answer is option 2: Standard - IA.

Option 1 is because the standard storage class is not cost-efficient in this scenario.

Option 3 is because the Intelligent Tiering storage class entails an additional fee for monitoring and automation of each object in your S3 bucket, compared to the Standard storage class and S3 Standard - Infrequent Access.

Amazon S3 Standard - Infrequent Access is an Amazon S3 storage class for data that is accessed less frequently, but requires rapid access when needed. Standard - IA offers the high durability, throughput, and low latency of Amazon S3 Standard, with a low per GB storage price and per GB retrieval fee.

This combination of low cost and high performance makes Standard - IA ideal for long-term storage, backups, and as a data store for disaster recovery. The Standard - IA storage class is set at the object level and can exist in the same bucket as Standard, allowing you to use lifecycle policies to automatically transition objects between storage classes without any application changes.

Question 34:

An On-Demand EC2 instance is launched into a VPC subnet with the Network ACL configured to allow all inbound traffic and deny all outbound traffic. The instance's security group has an inbound rule to allow SSH from any IP address and does not have any outbound rules.

In this scenario, what are the changes needed to allow SSH connection to the instance?

A. The outbound security group needs to be modified to allow outbound traffic. ()
B. The outbound network ACL needs to be modified to allow outbound traffic.(Correct).
C. No action needed. It can already be accessed from any IP address using SSH.
D. Both the outbound security group and outbound network ACL need to be modified to allow outbound traffic.

EXPLANATION

In order for you to establish an SSH connection from your home computer to your EC2 instance, you need to do the following:

• On the Security Group, add an Inbound Rule to allow SSH traffic to your EC2 instance.

- On the NACL, add both an Inbound and Outbound Rule to allow SSH traffic to your EC2 instance.

The reason why you have to add both Inbound and Outbound SSH rule is due to the fact that Network ACLs are stateless which means that responses to allow inbound traffic are subject to the rules for outbound traffic (and vice versa). In other words, if you only enabled an Inbound rule in NACL, the traffic can only go in but the SSH response will not go out since there is no Outbound rule.

Security groups are stateful which means that if an incoming request is granted, then the outgoing traffic will be automatically granted as well, regardless of the outbound rules.

Question 35:

An investment bank has a distributed batch processing application which is hosted in an Auto Scaling group of Spot EC2 instances with an SQS queue. You configured your components to use client-side buffering so that the calls made from the client will be buffered first and then sent as a batch request to SQS. What is a period of time during which the SQS queue prevents other consuming components from receiving and processing a message?

A. Component Timeout()
B. Visibility Timeout(Correct)
C. Processing Timeout
D. Receiving Timeout

EXPLANATION

The visibility timeout is a period of time during which Amazon SQS prevents other consuming components from receiving and processing a message.

When a consumer receives and processes a message from a queue, the message remains in the queue. Amazon SQS doesn't automatically delete the message. Because Amazon SQS is a distributed system, there's no guarantee that the consumer actually receives the message (for example, due to a connectivity issue, or due to an issue in the consumer application). Thus, the consumer must delete the message from the queue after receiving and processing it.

Immediately after the message is received, it remains in the queue. To prevent other consumers from processing the message again, Amazon SQS sets a visibility timeout, a period of time during which Amazon SQS prevents other consumers from receiving and processing the message. The default visibility timeout for a message is 30 seconds. The maximum is 12 hours.

Question 36:

You are consulted by a multimedia company that needs to deploy web services to an AWS region which they have never used before. The company currently has an IAM role for their Amazon EC2 instance which permits the instance to access Amazon DynamoDB. They want their EC2 instances in the new region to have the exact same privileges.

What should you do to accomplish this?

A. In the new Region, create a new IAM role and associated policies then assign it to the new instance.
B. Assign the existing IAM role to instances in the new region.(Correct)
C. Duplicate the IAM role and associated policies to the new region and attach it to the instances.
D. Create an Amazon Machine Image (AMI) of the instance and copy it to the new region.

EXPLANATION

In this scenario, the company has an existing IAM role hence you don't need to create a new one. IAM roles are global service that are available to all regions hence, all you have to do is assign the existing IAM role to the instance in the new region.

Option 1 is because you don't need to create another IAM role - there is already an existing one.

Option 3 is as you don't need duplicate IAM roles for each region. One IAM role suffices for the instances on two regions.

Option 4 is because creating an AMI image does not affect the IAM role of the instance.

Question 37:

A financial company wants to store their data in Amazon S3 but at the same time, they want to store their frequently accessed data locally on their on-premises server. This is due to the fact that they do not have the option to extend their on-premises storage, which is why they are looking for a durable and scalable storage service to use in AWS.

What is the best solution for this scenario?

A. Use a fleet of EC2 instance with EBS volumes to store the commonly used data.()
B. Use both Elasticache and S3 for frequently accessed data.
C. Use the Amazon Storage Gateway - Cached Volumes.(Correct)
D. Use Amazon Glacier.

EXPLANATION

By using Cached volumes, you store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally in your on-premises network. Cached volumes offer substantial cost savings on primary storage and minimize the need to scale your storage on-premises. You also retain

low-latency access to your frequently accessed data. This is the best solution for this scenario.

Option 1 is because an EC2 instance is not a storage service and it does not provide the required durability and scalability.

Option 2 is as storing frequently accessed data on both Elasticache and S3 is not efficient. Moreover, the question explicitly said that the frequently accessed data should be stored locally on their on-premises server and not on AWS.

Option 4 is as Amazon Glacier is mainly used for data archiving.

Question 38:

You are working as a Solutions Architect for a leading technology company where you are instructed to troubleshoot the operational issues of your cloud architecture by logging the AWS API call history of your AWS resources. You need to quickly identify the most recent changes made to resources in your environment, including creation, modification, and deletion of AWS resources. One of the requirements is that the generated log files should be encrypted to avoid any security issues.

Which of the following is the most suitable approach to implement the encryption?

A. Use CloudTrail and configure the destination Amazon Glacier archive to use Server-Side Encryption (SSE).
B. Use CloudTrail and configure the destination S3 bucket to use Server-Side Encryption (SSE).()
C. Use CloudTrail and ensure that the Server-Side Encryption (SSE) option is enabled for the trail in the CloudTrail console.
D. Use CloudTrail with its default settings(Correct)

EXPLANATION

By default, CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encrypt your log files with an AWS Key Management Service (AWS KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about log file delivery and validation, you can set up Amazon SNS notifications.

Option 1 is because CloudTrail stores the log files to S3 and not in Glacier. Take note that by default, CloudTrail event log files are already encrypted using Amazon S3 server-side encryption (SSE).

Option 2 is because CloudTrail event log files are already encrypted using the Amazon S3 server-side encryption (SSE) which is why you do not have to do this anymore.

Option 3 is because there is no available Server-Side Encryption (SSE) option in the CloudTrail console.

Question 39:

You are running an EC2 instance store-based instance. You shut it down and then start the instance. You noticed that the data which you have saved earlier is no longer available.

What might be the cause of this?

A. The volume of the instance was not big enough to handle all of the processing data.
B. The EC2 instance was using EBS backed root volumes, which are ephemeral and only live for the life of the instance.
C. The EC2 instance was using instance store volumes, which are ephemeral and only live for the life of the instance.(Correct)
D. The instance was hit by a virus that wipes out all data.

EXPLANATION

An instance store provides temporary block-level storage for your instance. This storage is located on disks that are physically attached to the host computer. Instance store is ideal for temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers.

An instance store consists of one or more instance store volumes exposed as block devices. The size of an instance store as well as the number of devices available varies by instance type. While an instance store is dedicated to a particular instance, the disk subsystem is shared among instances on a host computer.

The data in an instance store persists only during the lifetime of its associated instance. If an instance reboots (intentionally or unintentionally), data in the instance store persists. However, data in the instance store is lost under the following circumstances:

- The underlying disk drive fails
- The instance stops
- The instance terminates

Question 40:

You are planning to migrate a MySQL database from your on-premises data center to your AWS Cloud. This database will be used by a legacy batch application which has steady-state workloads in the morning but has its peak load at night for the end-of-day processing. You need to choose an EBS volume which can handle a maximum of 450 GB of data and can also be used as the system boot volume for your EC2 instance.

Which of the following is the most cost-effective storage type to use in this scenario?

- **A.** Amazon EBS Provisioned IOPS SSD()
- B. Amazon EBS Throughput Optimized HDD
- **C. Amazon EBS General Purpose SSD(Correct)**
- D. Amazon EBS Cold HDD

EXPLANATION

In this scenario, a legacy batch application which has steady-state workloads requires a relational MySQL database. The EBS volume that you should use has to handle a maximum of 450 GB of data and can also be used as the system boot volume for your EC2 instance. Since HDD volumes cannot be used as a bootable volume, we can narrow down our options by selecting SSD volumes. In addition, SSD volumes are more suitable for transactional database workloads, as shown in the table below:

General Purpose SSD (gp2) volumes offer cost-effective storage that is ideal for a broad range of workloads. These volumes deliver single-digit millisecond latencies and the ability to burst to 3,000 IOPS for extended periods of time. Between a minimum of 100 IOPS (at 33.33 GiB and below) and a maximum of 10,000 IOPS (at 3,334 GiB and above), baseline performance scales linearly at 3 IOPS per GiB of volume size. AWS designs gp2 volumes to deliver the provisioned performance 99% of the time. A gp2 volume can range in size from 1 GiB to 16 TiB.

Option 1 is because Amazon EBS Provisioned IOPS SSD is not the most cost-effective EBS type and is primarily used for critical business applications that require sustained IOPS performance.

Option 2 is because Amazon EBS Throughput Optimized HDD is primarily used for frequently accessed, throughput-intensive workloads. Although it is a low-cost HDD volume, it cannot be used as a system boot volume.

Option 4 is because although Amazon EBS Cold HDD provides lower cost HDD volume compared to General Purpose SSD, it cannot be used as a system boot volume.

Question 41:

You are a working as a Solutions Architect for a fast-growing startup which just started operations during the past 3 months. They currently have an on-premises Active Directory and 10 computers. To save costs in procuring physical workstations, they decided to deploy virtual desktops for their new employees in a virtual private cloud in AWS. The new cloud infrastructure

should leverage on the existing security controls in AWS but can still communicate with their on-premises network.

Which set of AWS services will you use to meet these requirements?

A. AWS Directory Services, VPN connection, and ClassicLink
B. AWS Directory Services, VPN connection, and Amazon Workspaces(Correct)
C. AWS Directory Services, VPN connection, and AWS Identity and Access Management ().
D. AWS Directory Services, VPN connection, and Amazon S3

EXPLANATION

For this scenario, the best choice is Option 2: AWS Directory Services, VPN connection, and Amazon Workspaces. First, you need a VPN connection to connect the VPC and your on-premises network. Second, you need AWS Directory Services to integrate with your on-premises Active Directory and lastly, you need to use Amazon Workspace to create the needed virtual desktops in your VPC.

Question 42:

A loan processing application is hosted in a single On-Demand EC2 instance in your VPC. To improve the scalability of your application, you have to use Auto Scaling to automatically add new EC2 instances to handle a surge of incoming requests.

Which of the following items should be done in order to add an existing EC2 instance to an Auto Scaling group?

A. You must stop the instance first.
B. You have to ensure that the AMI used to launch the instance still exists.(Correct)
C. You have to ensure that the AMI used to launch the instance no longer exists.
D. The instance is launched into one of the Availability Zones defined in your Auto Scaling group.(Correct)
E. You have to ensure that the instance is in a different Availability Zone as the Auto Scaling group.

EXPLANATION

Amazon EC2 Auto Scaling provides you with an option to enable automatic scaling for one or more EC2 instances by attaching them to your existing Auto Scaling group. After the instances are attached, they become a part of the Auto Scaling group.

The instance that you want to attach must meet the following criteria:

- The instance is in the running state.

- The AMI used to launch the instance must still exist.

- The instance is not a member of another Auto Scaling group.

- The instance is launched into one of the Availability Zones defined in your Auto Scaling group.

- If the Auto Scaling group has an attached load balancer, the instance and the load balancer must both be in EC2-Classic or the same VPC. If the Auto Scaling group has an attached target group, the instance and the load balancer must both be in the same VPC.

Based on the above criteria, Options 2 and 4 are the correct answers.

Question 43:

You are working for a large financial company. In their enterprise application, they want to apply a group of database-specific settings to their Relational Database Instances.

Which of the following options can be used to easily apply the settings in one go for all of the Relational database instances?

A. Security Groups
B. NACL Groups
C. Parameter Groups(Correct)
D. IAM Roles()

EXPLANATION

You manage your DB engine configuration through the use of parameters in a DB parameter group. DB parameter groups act as a container for engine configuration values that are applied to one or more DB instances.

Question 44:

A client is hosting their company website on a cluster of web servers that are behind a public-facing load balancer. The client also uses Amazon Route 53 to manage their public DNS.

How should the client configure the DNS zone apex record to point to the load balancer?

A. Create an A record pointing to the IP address of the load balancer.
B. Create a CNAME record pointing to the load balancer DNS name.
C. Create an alias for CNAME record to the load balancer DNS name.()
D. Create an A record aliased to the load balancer DNS name.(Correct)

EXPLANATION

Route 53's DNS implementation connects user requests to infrastructure running inside (and outside) of Amazon Web Services (AWS). For example, if you have

multiple web servers running on EC2 instances behind an Elastic Load Balancing load balancer, Route 53 will route all traffic addressed to your website (e.g. www.tutorialsdojo.com) to the load balancer DNS name (e.g. elbtutorialsdojo123.elb.amazonaws.com).

Additionally, Route 53 supports the alias resource record set, which lets you map your zone apex (e.g. tutorialsdojo.com) DNS name to your load balancer DNS name. IP addresses associated with Elastic Load Balancing can change at any time due to scaling or software updates. Route 53 responds to each request for an Alias resource record set with one IP address for the load balancer.

Option 1 is . You should be using an Alias record pointing to the DNS name of the load balancer since the IP address of the load balancer can change at any time.

Option 2 and 3 are because CNAME records cannot be created for your zone apex. You should create an alias record at the top node of a DNS namespace which is also known as the zone apex. For example, if you register the DNS name tutorialsdojo.com, the zone apex is tutorialsdojo.com. You can't create a CNAME record directly for tutorialsdojo.com, but you can create an alias record for tutorialsdojo.com that routes traffic to www.tutorialsdojo.com.

Question 45:

You recently launched a news website which is expected to be visited by millions of people around the world. You chose to deploy the website in AWS to take advantage of its extensive range of cloud services and global infrastructure. Aside from AWS Region and Availability Zones, which of the following is part of the AWS Global Infrastructure that is used for content distribution?

A. Edge Location (Correct)
B. Bastion Hosts
C. Hypervisor()
D. VPC Endpoint
E. EXPLANATION

An edge location helps deliver high availability, scalability, and performance of your application for all of your customers from anywhere in the world. This is used by other services such as Lambda and Amazon CloudFront.

Amazon CloudFront is a web service that gives businesses and web application developers an easy and cost-effective way to distribute content with low latency and high data transfer speeds. CloudFront delivers your files to end-users using a global network of edge locations.

Option 2 is because a bastion host is not part of the AWS Global Infrastructure. It is just a host computer or a "jump server" used to allow SSH access to your EC2 instances from an outside network.

Option 3 is because a hypervisor is just a computer software, firmware or hardware that creates and runs virtual machines. This technology relates to EC2 instances but it is not part of the AWS Global Infrastructure.

Option 4 is because VPC Endpoint is not part of the AWS Global Infrastructure and is just used to privately connect your VPC to other AWS services and endpoint services.

Question 46:

You are setting up a cost-effective architecture for a log processing application which has frequently accessed, throughput-intensive workloads. The application should be hosted in an On-Demand EC2 instance in your VPC.

Which of the following is the most suitable EBS volume type to use in this scenario?

A. EBS Provisioned IOPS SSD
B. EBS Throughput Optimized HDD (Correct)
C. EBS General Purpose SSD
D. EBS Cold HDD

EXPLANATION

In the exam, always consider the difference between SSD and HDD as shown on the table below. This will allow you to easily eliminate specific EBS-types in the options which are not SSD or not HDD, depending on whether the question asks for a storage type which has small, random I/O operations or large, sequential I/O operations.

Since the scenario has workloads with large, sequential I/O operations, we can narrow down our options by selecting HDD volumes, instead of SDD volumes which are more suitable for small, random I/O operations.

Throughput Optimized HDD (st1) volumes provide low-cost magnetic storage that defines performance in terms of throughput rather than IOPS. This volume type is a good fit for large, sequential workloads such as Amazon EMR, ETL, data warehouses, and log processing. Bootable st1 volumes are not supported.

Throughput Optimized HDD (st1) volumes, though similar to Cold HDD (sc1) volumes, are designed to support frequently accessed data.

Option 1 is because Amazon EBS Provisioned IOPS SSD is not the most cost-effective EBS type and is primarily used for critical business applications that require sustained IOPS performance.

Option 3 is because although an Amazon EBS General Purpose SSD volume balances price and performance for a wide variety of workloads, it is not suitable for frequently accessed, throughput-intensive workloads. Throughput Optimized HDD is a more suitable option to use than General Purpose SSD.

Option 4 is because although Amazon EBS Cold HDD provides lower cost HDD volume compared to General Purpose SSD, it is much suitable for lessfrequently accessed workloads.

Question 47:

You have a web application running on EC2 instances which processes sensitive financial information. All of the data are stored on an Amazon S3 bucket. The financial information is accessed by users over the Internet. The security team of the company is concerned that the Internet connectivity to Amazon S3 is a security risk. In this scenario, what will you do to resolve this security concern?

A. **Change the web architecture to access the financial data through a Gateway VPC Endpoint. (Correct)**
B. Change the web architecture to access the financial data in your S3 bucket through a VPN connection.()
C. Change the web architecture to access the financial data hosted in your S3 bucket by creating a custom VPC endpoint service.
D. Change the web architecture to access the financial data in S3 through an interface VPC endpoint, which is powered by AWS PrivateLink.

EXPLANATION

Take note that your VPC lives within a larger AWS network and the services, such as S3, DynamoDB, RDS and many others, are located outside of your VPC, but still within the AWS network. By default, the connection that your VPC uses to connect to your S3 bucket or any other service traverses the public Internet via your Internet Gateway.

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.

There are two types of VPC endpoints: interface endpoints and gateway endpoints. You have to create the type of VPC endpoint required by the supported service.

An interface endpoint is an elastic network interface with a private IP address that serves as an entry point for traffic destined to a supported service. A gateway endpoint is a gateway that is a target for a specified route in your route table, used for traffic destined to a supported AWS service. It is important to note that for Amazon S3 and DynamoDB service, you have to create a gateway endpoint and then use an interface endpoint for other services.

Option 2 is because a VPN connection still goes through the public Internet. You have to use a VPC Endpoint in this scenario and not VPN, to privately connect your VPC to supported AWS services such as S3.

Option 3 is because a "VPC endpoint service" is quite different from a "VPC endpoint". With VPC endpoint service, you are the service provider where you can create your own application in your VPC and configure it as an AWS PrivateLink-powered service (referred to as an endpoint service). Other AWS principals can create a connection from their VPC to your endpoint service using an interface VPC endpoint.

Option 4 is because although you are correctly using a VPC Endpoint to satisfy the requirement, you chose a wrong type of VPC Endpoint. Remember that for S3 and

DynamoDB service, you have to use a Gateway VPC Endpoint and not an Interface VPC Endpoint.

Question 48:

You have an On-Demand EC2 instance with an attached EBS volume. There is a scheduled job that creates a snapshot of this EBS volume every midnight at 12 AM when the instance is not used. One night, there has been a production incident where you need to perform a change on both the instance and on the EBS volume at the same time, when the snapshot is currently taking place.

Which of the following scenario is true when it comes to the usage of an EBS volume while the snapshot is in progress?

- **A. The EBS volume can be used while the snapshot is in progress.(Correct)**
- B. The EBS volume cannot be detached or attached to an EC2 instance until the snapshot completes()
- C. The EBS volume can be used in read-only mode while the snapshot is in progress.
- D. The EBS volume cannot be used until the snapshot completes.

EXPLANATION

Snapshots occur asynchronously; the point-in-time snapshot is created immediately, but the status of the snapshot is pending until the snapshot is complete (when all of the modified blocks have been transferred to Amazon S3), which can take several hours for large initial snapshots or subsequent snapshots where many blocks have changed.

While it is completing, an in-progress snapshot is not affected by ongoing reads and writes to the volume hence, you can still use the EBS volume normally.

When you create an EBS volume based on a snapshot, the new volume begins as an exact replica of the original volume that was used to create the snapshot. The replicated volume loads data lazily in the background so that you can begin using it immediately. If you access data that hasn't been loaded yet, the volume immediately downloads the requested data from Amazon S3, and then continues loading the rest of the volume's data in the background.

Question 49:

The start-up company that you are working for has a batch job application that is currently hosted on an EC2 instance. It is set to process messages from a queue created in SQS with default settings. You configured the application to process the messages once a week. After 2 weeks, you noticed that not all messages are being processed by the application.

What is the root cause of this issue?

- A. The batch job application is configured to long polling.
- **B. Amazon SQS has automatically deleted the messages that have been in a queue for more than the maximum message retention period.(Correct)**

C. The SQS queue is set to short-polling.
D. Missing permissions in SQS.

EXPLANATION

Amazon SQS automatically deletes messages that have been in a queue for more than the maximum message retention period. The default message retention period is 4 days. Since the queue is configured to the default settings and the batch job application only processes the messages once a week, the messages that are in the queue for more than 4 days are deleted. This is the root cause of the issue.

To fix this, you can increase the message retention period to a maximum of 14 days using the SetQueueAttributes action.

Question 50:

You just joined a large tech company with an existing Amazon VPC. When reviewing the Auto Scaling events, you noticed that their web application is scaling up and down multiple times within the hour.

What design change could you make to optimize cost while preserving elasticity?

A. Change the cooldown period of the Auto Scaling group and set the CloudWatch metric to a higher threshold(Correct)
B. Increase the instance type in the launch configuration()
C. Increase the base number of Auto Scaling instances for the Auto Scaling group
D. Add provisioned IOPS to the instances
E. Add EBS Volumes to the instances

EXPLANATION

Since the application is scaling up and down multiple times within the hour, the issue lies on the cooldown period of the Auto Scaling group.

The cooldown period is a configurable setting for your Auto Scaling group that helps to ensure that it 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, it 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, the Auto Scaling group does not wait for the cooldown period to complete before replacing the unhealthy instance.

Question 51:

A health organization is using a large Dedicated EC2 instance with multiple EBS volumes to host its health records web application. The EBS volumes must be encrypted due to the confidentiality of the data that they are handling and also to comply with the HIPAA (Health Insurance Portability and Accountability Act) standard.

In EBS encryption, what service does AWS use to secure the volume's data at rest?

- **A. By using your own keys in AWS Key Management Service (KMS).(Correct)**
- B. By using S3 Server-Side Encryption.
- **C. By using Amazon-managed keys in AWS Key Management Service (KMS).(Correct)**
- D. By using S3 Client-Side Encryption.
- E. By using a password stored in CloudHSM.
- F. By using the SSL certificates provided by the AWS Certificate Manager (ACM).

EXPLANATION

Amazon EBS encryption offers seamless encryption of EBS data volumes, boot volumes, and snapshots, eliminating the need to build and maintain a secure key management infrastructure. EBS encryption enables data at rest security by encrypting your data using Amazon-managed keys, or keys you create and manage using the AWS Key Management Service (KMS). The encryption occurs on the servers that host EC2 instances, providing encryption of data as it moves between EC2 instances and EBS storage. Hence, options 1 and 3 are the right answers.

Options 2 and 4 are as these relate only to S3.

Option 5 is as you only store keys in CloudHSM and not passwords.

Option 6 is as ACM only provides SSL certificates and not data encryption of EBS Volumes.

Question 52:

You are required to deploy a Docker-based batch application to your VPC in AWS. The application will be used to process both mission-critical data as well as non-essential batch jobs. Which of the following is the most cost-effective option to use in implementing this architecture?

- **A. Use ECS as the container management service then set up a combination of Reserved and Spot EC2 Instances for processing mission-critical and non-essential batch jobs respectively. (Correct)**
- B. Use ECS as the container management service then set up Reserved EC2 Instances for processing both mission-critical and non-essential batch jobs. ()
- C. Use ECS as the container management service then set up On-Demand EC2 Instances for processing both mission-critical and non-essential batch jobs.
- D. Use ECS as the container management service then set up Spot EC2 Instances for processing both mission-critical and non-essential batch jobs.

EXPLANATION

Amazon ECS lets you run batch workloads with managed or custom schedulers on Amazon EC2 On-Demand Instances, Reserved Instances, or Spot Instances. You can launch a combination of EC2 instances to set up a cost-effective architecture depending on your workload. You can launch Reserved EC2 instances to process the mission-critical data and Spot EC2 instances for processing non-essential batch jobs.

There are two different charge models for Amazon Elastic Container Service (ECS): Fargate Launch Type Model and EC2 Launch Type Model. With Fargate, you pay for the amount of vCPU and memory resources that your containerized application requests while for EC2 launch type model, there is no additional charge. You pay for AWS resources (e.g. EC2 instances or EBS volumes) you create to store and run your application. You only pay for what you use, as you use it; there are no minimum fees and no upfront commitments.

Option 2 is because processing the non-essential batch jobs can be handled much cheaper by using Spot EC2 instances instead of Reserved Instances.

Option 3 is because an On-Demand instance costs more compared to Reserved and Spot EC2 instances. Processing the non-essential batch jobs can be handled much cheaper by using Spot EC2 instances instead of On-Demand instances.

Option 4 is because although this set up provides the cheapest solution among other options, it will not be able to meet the required workload. Using Spot instances to process mission-critical workloads is not suitable since these types of instances can be terminated by AWS at any time, which can affect critical processing.

Question 53:

A website is running on an Auto Scaling group of On-Demand EC2 instances which are abruptly getting terminated from time to time. To automate the monitoring process, you started to create a simple script which uses the AWS CLI to find the root cause of this issue.

Which of the following is the most suitable command to use?

- **A. aws ec2 describe-instances(Correct)**
- B. aws ec2 describe-images
- C. aws ec2 get-console-screenshot
- D. aws ec2 describe-volume-status

EXPLANATION

The describe-instances command shows the status of the EC2 instances including the recently terminated instances. It also returns a StateReason of why the instance was terminated.

Question 54:

Your manager instructed you to use Route 53 instead of an ELB to load balance the incoming request to your web application. The system is deployed to two EC2 instances to which the traffic needs to be distributed to. You want to set a specific percentage of traffic to go to each instance.

Which routing policy would you use?

A. Latency
B. Failover
C. Weighted(Correct)
D. Geolocation

EXPLANATION

Weighted routing lets you associate multiple resources with a single domain name (example.com) or subdomain name (acme.example.com) and choose how much traffic is routed to each resource. This can be useful for a variety of purposes including load balancing and testing new versions of software. You can set a specific percentage of how much traffic will be allocated to the resource by specifying the weights.

For example, if you want to send a tiny portion of your traffic to one resource and the rest to another resource, you might specify weights of 1 and 255. The resource with a weight of 1 gets 1/256th of the traffic (1/1+255), and the other resource gets 255/256ths (255/1+255).

You can gradually change the balance by changing the weights. If you want to stop sending traffic to a resource, you can change the weight for that record to 0.

Question 55:

An online stock trading portal is deployed in AWS and in order to complete the set up, you need to offload the SSL/TLS processing for your web servers using CloudHSM. This will reduce the burden on your web servers and provides extra security by storing your web server's private key in this cloud-based hardware security module.

Which of the following statements is not true about Amazon CloudHSM?

A. AWS manages the hardware security module (HSM) appliance, but does not have access to your keys.()
B. Your HSMs are in your Virtual Private Cloud (VPC) and isolated from other AWS networks.
C. You control and manage your own encryption keys.
D. It provides a secure key storage in tamper-resistant hardware available in a single Availability Zone.(Correct)

EXPLANATION

Take note that CloudHSM provides a secure key storage in tamper-resistant hardware available in multiple Availability Zones (AZs) and not just on one AZ. Hence, Option 4 is the answer.

AWS CloudHSM runs in your own Amazon Virtual Private Cloud (VPC), enabling you to easily use your HSMs with applications running on your Amazon EC2 instances. With CloudHSM, you can use standard VPC security controls to manage access to your HSMs.

Your applications connect to your HSMs using mutually authenticated SSL channels established by your HSM client software. Since your HSMs are located in Amazon datacenters near your EC2 instances, you can reduce the network latency between your applications and HSMs versus an on-premises HSM.

- AWS manages the hardware security module (HSM) appliance but does not have access to your keys
- You control and manage your own keys
- Application performance improves (due to close proximity with AWS workloads)
- Secure key storage in tamper-resistant hardware available in multiple Availability Zones (AZs)
- Your HSMs are in your Virtual Private Cloud (VPC) and isolated from other AWS networks.

Separation of duties and role-based access control is inherent in the design of the AWS CloudHSM. AWS monitors the health and network availability of your HSMs but is not involved in the creation and management of the key material stored within your HSMs. You control the HSMs and the generation and use of your encryption keys.

Question 56:

The social media company that you are working for needs to capture the detailed information of all HTTP requests that went through their public-facing application load balancer every five minutes. They want to use this data for analyzing traffic patterns and for troubleshooting their web applications in AWS.

Which of the following options meet the customer requirements?

A. Enable AWS CloudTrail for their application load balancer.()
B. **Enable access logs on the application load balancer.(Correct**)
C. Add an Amazon CloudWatch Logs agent on the application load balancer.
D. Enable Amazon CloudWatch metrics on the application load balancer.

EXPLANATION

Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and troubleshoot issues.

Access logging is an optional feature of Elastic Load Balancing that is disabled by default. After you enable access logging for your load balancer, Elastic Load Balancing captures the logs and stores them in the Amazon S3 bucket that you specify as compressed files. You can disable access logging at any time.

Question 57:

You are a Solutions Architect working for a startup which is currently migrating their production environment to AWS. Your manager asked you to set up access to the AWS console using Identity Access Management (IAM). You have created 5 users for your system administrators.

What further steps do you need to take to enable your system administrators to get access to the AWS console?

A. Provide the system administrators the secret access key and access key id.
B. Enable multi-factor authentication on their accounts and define a password policy.()
C. Provide a password for each user created and give these passwords to your system administrators.(Correct)
D. Add the administrators to the Security Group.

EXPLANATION

The AWS Management Console is the web interface used to manage your AWS resources using your web browser. To access this, your users should have a password that they can use to login to the web console.

Option 1 is as the secret access key and access key id are used to trigger AWS API calls.

Option 2 is because the multi-factor authentication and a password policy are just additional security measures for the IAM user but these won't enable them to access the AWS Management Console.

Option 4 is as you could not add an IAM user to a security group. Remember that a security group is used for EC2 instances only.

Question 58:

You have just launched a new API Gateway service which uses AWS Lambda as a serverless computing service. In what type of protocol will your API endpoint be exposed?

A. HTTP/2
B. HTTPS(Correct)
C. HTTP()
D. WebSocket

EXPLANATION

All of the APIs created with Amazon API Gateway expose HTTPS endpoints only. Amazon API Gateway does not support unencrypted (HTTP) endpoints. By default,

Amazon API Gateway assigns an internal domain to the API that automatically uses the Amazon API Gateway certificate. When configuring your APIs to run under a custom domain name, you can provide your own certificate for the domain.

Question 59:

An application is hosted in an On-Demand EC2 instance and is using Amazon SDK to communicate to other AWS services such as S3, DynamoDB, and many others. As part of the upcoming IT audit, you need to ensure that all API calls to your AWS resources are logged and durably stored.

Which is the most suitable service that you should use to meet this requirement?

A. Amazon CloudWatch
B. AWS CloudTrail(Correct)
C. AWS X-Ray
D. Amazon API Gateway

EXPLANATION

AWS CloudTrail increases visibility into your user and resource activity by recording AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred.

Option 1 is because Amazon CloudWatch is primarily used for systems monitoring based on the server metrics. It does not have the capability to track API calls to your AWS resources.

Option 3 is because AWS X-Ray is usually used to debug and analyze your microservices applications with request tracing so you can find the root cause of issues and performance. Unlike CloudTrail, it does not record the API calls that were made to your AWS resources.

Option 4 is because Amazon API Gateway is not used for logging each and every API call to your AWS resources. It is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale.

Question 60:

You are working as a Principal Solutions Architect for a leading digital news company which has both an on-premises data center as well as an AWS cloud infrastructure. They store their graphics, audios, videos, and other multimedia assets primarily in their on-premises storage server and uses an S3 Standard storage class bucket as a backup. Their data are heavily used for only a week (7 days) but after that period, it will be infrequently used by their customers. You are instructed to save storage costs in AWS yet maintain the ability to immediately fetch their media assets for a surprise annual data audit.

Which of the following options should you implement to meet the above requirement?

A. **Set a lifecycle policy in the bucket to transition the data to Glacier after one week (7 days).(Correct)**
B. Set a lifecycle policy in the bucket to transition the data to S3 - Standard IA storage class after one week (7 days).()
C. Set a lifecycle policy in the bucket to transition the data to S3 - One Zone-Infrequent Access storage class after one week (7 days).
D. **Set a lifecycle policy in the bucket to transition to S3 - Standard IA after 30 days(Correct)**

EXPLANATION

You can add rules in a lifecycle configuration to tell Amazon S3 to transition objects to another Amazon S3 storage class. For example: When you know that objects are infrequently accessed, you might transition them to the STANDARD_IA storage class. Or transition your data to the GLACIER storage class in case you want to archive objects that you don't need to access in real time.

In a lifecycle configuration, you can define rules to transition objects from one storage class to another to save on storage costs. When you don't know the access patterns of your objects or your access patterns are changing over time, you can transition the objects to the INTELLIGENT_TIERING storage class for automatic cost savings.

The lifecycle storage class transitions have a constraint when you want to transition from the STANDARD storage classes to either STANDARD_IA or ONEZONE_IA. The following constraints apply:

- For larger objects, there is a cost benefit for transitioning to STANDARD_IA or ONEZONE_IA. Amazon S3 does not transition objects that are smaller than 128 KB to the STANDARD_IA or ONEZONE_IA storage classes because it's not cost effective.

- Objects must be stored at least 30 days in the current storage class before you can transition them to STANDARD_IA or ONEZONE_IA. For example, you cannot create a lifecycle rule to transition objects to the STANDARD_IA storage class one day after you create them. Amazon S3 doesn't transition objects within the first 30 days because newer objects are often accessed more frequently or deleted sooner than is suitable for STANDARD_IA or ONEZONE_IA storage.

- If you are transitioning noncurrent objects (in versioned buckets), you can transition only objects that are at least 30 days noncurrent to STANDARD_IA or ONEZONE_IA storage.

Since there is a time constraint in transitioning objects in S3, you can only change the storage class of your objects from S3 Standard storage class to STANDARD_IA or ONEZONE_IA storage after 30 days. This limitation does not apply on INTELLIGENT_TIERING, GLACIER, and DEEP_ARCHIVE storage class. In this scenario, you can set a lifecycle policy in the bucket to transition to S3 - Standard IA

after 30 days or alternatively, you can directly transition your data to Glacier after one week (7 days).

In addition, the requirement says that the media assets should be fetched immediately for a surprise annual data audit. This means that the retrieval will only happen once a year. You can use expedited retrievals in Glacier which will allow you to quickly access your data (within 1–5 minutes) when occasional urgent requests for a subset of archives are required. Hence, Options 1 and 5 are the correct answers.

Options 2 and 3 are both because there is a constraint in S3 that objects must be stored at least 30 days in the current storage class before you can transition them to STANDARD_IA or ONEZONE_IA. You cannot create a lifecycle rule to transition objects to either STANDARD_IA or ONEZONE_IA storage class 7 days after you create them because you can only do this after the 30-day period has elapsed. Hence, these options are .

Option 4 is because although DEEP_ARCHIVE storage class provides the most cost-effective storage option, it does not have the ability to do expedited retrievals, unlike Glacier. In the event that the surprise annual data audit happens, it may take several hours before you can retrieve your data.

Question 61:

Your company has a web-based ticketing service that utilizes Amazon SQS and a fleet of EC2 instances. The EC2 instances that consume messages from the SQS queue are configured to poll the queue as often as possible to keep end-to-end throughput as high as possible. You noticed that polling the queue in tight loops is using unnecessary CPU cycles, resulting in increased operational costs due to empty responses.

In this scenario, what will you do to make the system more cost-effective?

A. Configure Amazon SQS to use long polling by setting the ReceiveMessageWaitTimeSeconds to zero.
B. Configure Amazon SQS to use long polling by setting the ReceiveMessageWaitTimeSeconds to a number greater than zero.(Correct)
C. Configure Amazon SQS to use short polling by setting the ReceiveMessageWaitTimeSeconds to a number greater than zero.
D. Configure Amazon SQS to use short polling by setting the ReceiveMessageWaitTimeSeconds to zero.

EXPLANATION

In this scenario, the application is deployed in a fleet of EC2 instances that are polling messages from a single SQS queue. Amazon SQS uses short polling by default, querying only a subset of the servers (based on a weighted random distribution) to determine whether any messages are available for inclusion in the response. Short polling works for scenarios that require higher throughput. However, you can also configure the queue to use Long polling instead, to reduce cost.

The ReceiveMessageWaitTimeSeconds is the queue attribute that determines whether you are using Short or Long polling. By default, its value is zero which

means it is using Short polling. If it is set to a value greater than zero, then it is Long polling. Hence, Option 2 is correct.

Quick facts about SQS Long Polling:

- -Long polling helps reduce your cost of using Amazon SQS by reducing the number of empty responses when there are no messages available to return in reply to a ReceiveMessage request sent to an Amazon SQS queue and eliminating false empty responses when messages are available in the queue but aren't included in the response.
- -Long polling reduces the number of empty responses by allowing Amazon SQS to wait until a message is available in the queue before sending a response. Unless the connection times out, the response to the ReceiveMessage request contains at least one of the available messages, up to the maximum number of messages specified in the ReceiveMessage action.
- -Long polling eliminates false empty responses by querying all (rather than a limited number) of the servers. Long polling returns messages as soon any message becomes available.

Question 62:

A leading bank has an application that is hosted on an Auto Scaling group of EBS-backed EC2 instances. As the Solutions Architect, you need to provide the ability to fully restore the data stored in their EBS volumes by using EBS snapshots.

Which of the following approaches provide the lowest cost for Amazon Elastic Block Store snapshots?

A. Maintain two snapshots: the original snapshot and the latest incremental snapshot.()
B. Maintain a volume snapshot; subsequent snapshots will overwrite one another.
C. Just maintain a single snapshot of the EBS volume since the latest snapshot is both incremental and complete.(Correct)
D. Maintain the most current snapshot and then archive the original and incremental snapshots to Amazon Glacier.

EXPLANATION

To meet the requirement on this scenario, you can just maintain a single snapshot of the EBS volume since its latest snapshot is both incremental and complete.

You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots. Snapshots are incremental backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved. This minimizes the time required to create the snapshot and saves on storage costs by not duplicating data.

When you delete a snapshot, only the data unique to that snapshot is removed. Each snapshot contains all of the information needed to restore your data (from the moment the snapshot was taken) to a new EBS volume.

Question 63:

You are working for a large financial firm in the country. They have an AWS environment which contains several Reserved EC2 instances hosted in a web application that has been decommissioned last week. To save cost, you need to stop incurring charges for the Reserved instances as soon as possible.

What cost-effective steps will you take in this circumstance?

A. Stop the Reserved instances as soon as possible.
B. Contact AWS to cancel your AWS subscription.()
C. Go to the AWS Reserved Instance Marketplace and sell the Reserved instances.(Correct)
D. Terminate the Reserved instances as soon as possible to avoid getting billed at the on-demand price when it expires(Correct)
E. Go to the Amazon.com online shopping website and sell the Reserved instances.

EXPLANATION

The correct options are:

• Go to the AWS Reserved Instance Marketplace and sell the Reserved instances.

• Terminate the Reserved instances as soon as possible to avoid getting billed at the on-demand price when it expires

The Reserved Instance Marketplace is a platform that supports the sale of third-party and AWS customers' unused Standard Reserved Instances, which vary in terms of lengths and pricing options. For example, you may want to sell Reserved Instances after moving instances to a new AWS region, changing to a new instance type, ending projects before the term expiration, when your business needs change, or if you have unneeded capacity.

Option 1 is because a stopped instance can still be restarted. Take note that when a Reserved Instance expires, any instances that were covered by the Reserved Instance are billed at the on-demand price which costs significantly higher. Since the application is already decommissioned, there is no point of keeping the unused instances. It is also possible that there are associated Elastic IP addresses, which will incur charges if they are associated with stopped instances

Option 2 is as you don't need to close down your AWS account.

Option 5 is as you have to use AWS Reserved Instance Marketplace to sell your instances.

Question 64:

A local bank has an in-house application which handles sensitive financial data in a private subnet. After the data is processed by the EC2 worker instances, they will be delivered to S3 for ingestion by other services.

How should you design this solution so that the data does not pass through the public Internet?

A. Create an Internet gateway in the public subnet with a corresponding route entry that directs the data to S3.
B. Configure a VPC Interface Endpoint along with a corresponding route entry that directs the data to S3.()
C. Configure a VPC Endpoint Gateway along with a corresponding route entry that directs the data to S3.(Correct)
D. Provision a NAT gateway in the private subnet with a corresponding route entry that directs the data to S3.

EXPLANATION

The important concept that you have to understand in the scenario is that your VPC and your S3 bucket are located within the larger AWS network. However, the traffic coming from your VPC to your S3 bucket is traversing the public Internet by default. To better protect your data in transit, you can set up a VPC endpoint so the incoming traffic from your VPC will not pass through the public Internet, but instead through the private AWS network.

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 services do 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.

There are two types of VPC endpoints: interface endpoints and gateway endpoints. You should create the type of VPC endpoint required by the supported service. As a rule of thumb, most AWS services use VPC Interface Endpoint except for S3 and DynamoDB, which use VPC Gateway Endpoint.

Option 3 is correct because VPC Endpoint Gateway supports private connection to S3.

Option 1 is because Internet gateway is used for instances in the public subnet to have accessibility to the Internet.

Option 2 is because VPC Interface Endpoint does not support the S3 service. You should use a VPC Endpoint Gateway instead. As mentioned in the above

EXPLANATION, most AWS services use VPC Interface Endpoint except for S3 and DynamoDB, which use VPC Gateway Endpoint.

Option 4 is because NAT Gateway allows instances in the private subnet to gain access to the Internet, but not vice versa.

Question 65:

A data analytics company keeps a massive volume of data which they store in their on-premises data center. To scale their storage systems, they are looking for cloud-backed storage volumes that they can mount using Internet Small Computer System Interface (iSCSI) devices from their on-premises application servers. They have an on-site data analytics application which frequently access the latest data subsets locally while the older data are rarely accessed. You are required to minimize the need to scale the on-premises storage infrastructure while still providing their web application with low-latency access to the data.

A. **Which type of AWS Storage Gateway service will you use to meet the above requirements?**
B. Stored Volume Gateway()
C. Tape Gateway
D. **Cached Volume Gateway(Correct)**
E. File Gateway

EXPLANATION

In this scenario, the technology company is looking for a storage service that will enable their analytics application to frequently access the latest data subsets and not the entire data set because it was mentioned that the old data are rarely being used. This requirement can be fulfilled by setting up a Cached Volume Gateway in AWS Storage Gateway.

By using cached volumes, you can use Amazon S3 as your primary data storage, while retaining frequently accessed data locally in your storage gateway. Cached volumes minimize the need to scale your on-premises storage infrastructure, while still providing your applications with low-latency access to frequently accessed data. You can create storage volumes up to 32 TiB in size and afterwards, attach these volumes as iSCSI devices to your on-premises application servers. When you write to these volumes, your gateway stores the data in Amazon S3. It retains the recently read data in your on-premises storage gateway's cache and uploads buffer storage.

Cached volumes can range from 1 GiB to 32 TiB in size and must be rounded to the nearest GiB. Each gateway configured for cached volumes can support up to 32 volumes for a total maximum storage volume of 1,024 TiB (1 PiB).

In the cached volumes solution, AWS Storage Gateway stores all your on-premises application data in a storage volume in Amazon S3. Hence, the correct answer is Option 3.

Option 1 is because the requirement is to provide low latency access to the frequently accessed data subsets locally. Stored Volume Gateway is used if you need low-latency access to your entire dataset.

Option 2 is because a Tape Gateway is a cost-effective, durable, long-term offsite alternative for data archiving, which is not needed in this scenario.

Option 4 is because a File gateway does not provide you the required low-latency access to the frequently accessed data that the on-site analytics application needs.
