AWS Practise Question Paper-6

Question 1:

You are a Solutions Architect working for a software development company. You are planning to launch a fleet of EBS-backed EC2 instances and want to automatically assign each instance with a static private IP address which does not change even if the instances are restarted.

What should you do to accomplish this?

A. Launch the instances to a single Availability Zone.
B. Launch the instances to multiple Availability Zones.
C. Launch the instances in the Amazon Virtual Private Cloud (VPC).(Correct)
D. Launch the instances in a Placement Group.
E. Launch the instances in EC2-Classic.

EXPLANATION

In EC2-Classic, your EC2 instance receives a private IPv4 address from the EC2-Classic range each time it's started. In EC2-VPC on the other hand, your EC2 instance receives a static private IPv4 address from the address range of your default VPC. Hence, the correct answer is Option 3 and not Option 5.

Characteristic EC2-Classic Default VPC Nondefault VPC

Public IPv4 address (from Amazon's public IP address pool) Your instance receives a public IPv4 address from the EC2-Classic public IPv4 address pool. Your instance launched in a default subnet receives a public IPv4 address by default, unless you specify otherwise during launch, or you modify the subnet's public IPv4 address attribute. Your instance doesn't receive a public IPv4 address by default, unless you specify otherwise during launch, or you modify the subnet's public IPv4 address attribute.

Private IPv4 address Your instance receives a private IPv4 address from the EC2-Classic range each time it's started. Your instance receives a static private IPv4 address from the address range of your default VPC. Your instance receives a static private IPv4 address from the address range of your VPC.

Multiple private IPv4 addresses We select a single private IP address for your instance; multiple IP addresses are not supported. You can assign multiple private IPv4 addresses to your instance. You can assign multiple private IPv4 addresses to your instance.

Elastic IP address (IPv4) An Elastic IP is disassociated from your instance when you stop it. An Elastic IP remains associated with your instance when you stop it. An Elastic IP remains associated with your instance when you stop it.

Options 1 and 2 are due to the fact that Availability Zones do not provide static private IP addresses to EC2 instances.

Option 4 is as a Placement Group is just a grouping of instances.

Question 2:

A multinational corporate and investment bank is regularly processing steady workloads of accruals, loan interests, and other critical financial calculations every night at 10 PM to 3 AM on their on-premises data center for their corporate clients. Once the process is done, the results are then uploaded to the Oracle General Ledger which means that the processing should not be delayed nor interrupted. The CTO has decided to move their IT infrastructure to AWS to save cost and to improve the scalability of their digital financial services.

As the Senior Solutions Architect, how can you implement a cost-effective architecture in AWS for their financial system?

A. Use On-Demand EC2 instances which allows you to pay for the instances that you launch and use by the second.

B. Use Reserved Instances which provides a compute capacity that is always available for a term from one to three years.

C. Use Scheduled Reserved Instances which provides compute capacity that is always available on the specified recurring schedule, for a one-year term. (Correct)

D. Use Spot EC2 Instances launched by a persistent Spot request, which can significantly lower your Amazon EC2 costs.

E. Use Dedicated Hosts which provide a physical host that is fully dedicated to running your instances, and bring your existing per-socket, per-core, or per-VM software licenses to reduce costs.

F. Use Dedicated Instances that provide a compute capacity which runs on single-tenant hardware and are paid by the hour.

EXPLANATION

Scheduled Reserved Instances (Scheduled Instances) enable you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term. You reserve the capacity in advance, so that you know it is available when you need it. You pay for the time that the instances are scheduled, even if you do not use them.

Scheduled Instances are a good choice for workloads that do not run continuously, but do run on a regular schedule. For example, you can use Scheduled Instances for an application that runs during business hours or for batch processing that runs at the end of the week.

Question 3:

You are the Solutions Architect of a software development company where you are required to connect the on-premises infrastructure to their AWS cloud. Which of the following AWS service can you use to accomplish this? (Choose 3)

A. **IPsec VPN connection(Correct)**
B. Amazon Connect
C. **AWS Direct Connect(Correct)**
D. AWS On-Premises Connect
E. **AWS VPN CloudHub(Correct)**

EXPLANATION

You can connect your VPC to remote networks by using a VPN connection which can be Direct Connect, IPsec VPN connection, AWS VPN CloudHub, or a third party software VPN appliance. Hence, Options 1, 3 and 5 are correct.

Option 2 is because Amazon Connect is not a VPN connectivity option. It is actually a self-service, cloud-based contact center service in AWS that makes it easy for any business to deliver better customer service at lower cost. Amazon Connect is based on the same contact center technology used by Amazon customer service associates around the world to power millions of customer conversations.

Option 4 is as there is no such thing as AWS On-Premises Connect.

Question 4:

You are working as a Senior Solutions Architect in a digital media services startup. Your current project is about a movie streaming app where you are required to launch several EC2 instances on multiple availability zones. Which of the following will configure your load balancer to distribute incoming requests evenly to all EC2 instances across multiple Availability Zones?

A. Elastic Load Balancing request routing
B. An Amazon Route 53 weighted routing policy
C. **Cross-zone load balancing(Correct)**
D. An Amazon Route 53 latency routing policy
E. Elastic Load Balancing Redirects
F. An Amazon Route 53 failover routing policy

EXPLANATION

The right answer is to enable cross-zone load balancing.

If the load balancer nodes for your Classic Load Balancer can distribute requests regardless of Availability Zone, this is known as cross-zone load balancing. With cross-zone load balancing enabled, your load balancer nodes distribute incoming requests evenly across the Availability Zones enabled for your load balancer.

Otherwise, each load balancer node distributes requests only to instances in its Availability Zone.

For example, if you have 10 instances in Availability Zone us-west-2a and 2 instances in us-west-2b, the requests are distributed evenly across all 12 instances if cross-zone load balancing is enabled. Otherwise, the 2 instances in us-west-2b serve the same number of requests as the 10 instances in us-west-2a.

Cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled Availability Zone, and improves your application's ability to handle the loss of one or more instances. However, we still recommend that you maintain approximately equivalent numbers of instances in each enabled Availability Zone for higher fault tolerance.

Question 5:

An online stock trading system is hosted in AWS and uses an Auto Scaling group of EC2 instances, an RDS database, and an Amazon ElastiCache for Redis. You need to improve the data security of your in-memory data store by requiring the user to enter a password before they are granted permission to execute Redis commands.

Which of the following should you do to meet the above requirement?

A. Enable the in-transit encryption for Redis replication groups.
B. Create a new Redis replication group and set the AtRestEncryptionEnabled parameter to true.
C. Authenticate the users using Redis AUTH by creating a new Redis Cluster with both the --transit-encryption-enabled and --auth-token parameters enabled.(Correct)
D. Do nothing. This feature is already enabled by default.
E. None of the above.

EXPLANATION

Using Redis AUTH command can improve data security by requiring the user to enter a password before they are granted permission to execute Redis commands on a password-protected Redis server. Hence, Option 3 is the correct answer.

To require that users enter a password on a password-protected Redis server, include the parameter --auth-token with the correct password when you create your replication group or cluster and on all subsequent commands to the replication group or cluster.

Option 1 is because although in-transit encryption is part of the solution, it is missing the most important thing which is the Redis AUTH option.

Option 2 is because the Redis At-Rest Encryption feature only secures the data inside the in-memory data store. You have to use Redis AUTH option instead.

Option 4 is because the Redis AUTH option is disabled by default.

Question 6:

Your boss has asked you to launch a new MySQL RDS which ensures that you are available to recover from a database crash.

Which of the below is not a recommended practice for RDS?

A. Ensure that automated backups are enabled for the RDS
B. Use MyISAM as the storage engine for MySQL.(Correct)
C. Use InnoDB as the storage engine for MySQL.
D. Partition your large tables so that file sizes does not exceed the 16 TB limit.

EXPLANATION

Using MyISAM as the storage engine for MySQL is not recommended hence, this option is . The recommended storage engine for MySQL is InnoDB and not MyISAM.

Options 1, 3, and 4 are best practices in the AWS MySQL RDS documentation. Again, InnoDB is the recommended storage engine for MySQL. However, in case you require intense, full-text search capability, use MyISAM storage engine instead.

Question 7:

A fast food company is using AWS to host their online ordering system which uses an Auto Scaling group of EC2 instances deployed across multiple Availability Zones with an Application Load Balancer in front. To better handle the incoming traffic from various digital devices, you are planning to implement a new routing system where requests which have a URL of <server>/api/android are forwarded to one specific target group named "Android-Target-Group". Conversely, requests which have a URL of <server>/api/ios are forwarded to another separate target group named "iOS-Target-Group".

How can you implement this change in AWS?

A. Use host conditions to define rules that forward requests to different target groups based on the host name in the host header. This enables you to support multiple domains using a single load balancer.
B. Replace your ALB with a Classic Load Balancer then use path conditions to define rules that forward requests to different target groups based on the URL in the request.

C. **Use path conditions to define rules that forward requests to different target groups based on the URL in the request.(Correct)**
D. Replace your ALB with a Network Load Balancer then use host conditions to define rules that forward requests to different target groups based on the URL in the request.

EXPLANATION

You can use path conditions to define rules that forward requests to different target groups based on the URL in the request (also known as path-based routing). This type of routing is the most appropriate solution for this scenario hence, Option 3 is correct.

Each path condition has one path pattern. If the URL in a request matches the path pattern in a listener rule exactly, the request is routed using that rule.

A path pattern is case-sensitive, can be up to 128 characters in length, and can contain any of the following characters. You can include up to three wildcard characters.

- A–Z, a–z, 0–9
- _ - . $ / ~ " ' @ : +
- & (using &amp;)
- * (matches 0 or more characters)
- ? (matches exactly 1 character)

Example path patterns

- /img/*
- /js/*

Option 1 is because host-based routing defines rules that forward requests to different target groups based on the host name in the host header instead of the URL, which is what is needed in this scenario.

Option 2 is because a Classic Load Balancer does not support path-based routing. You must use an Application Load Balancer.

Option 4 is because a Network Load Balancer is used for applications that need extreme network performance and static IP. It also does not support path-based routing which is what is needed in this scenario. Furthermore, the statement mentions host-based routing yet, the description is about path-based routing.

Question 8:

You are working as a Solution Architect for a startup in Silicon Valley. Their application architecture is currently set up to store both the access key ID and the secret access key in a plain text file on a custom Amazon Machine Image (AMI). The EC2 instances, which are created by using this AMI, are using the stored access keys to connect to a DynamoDB table. What should you do to make the current architecture more secure?

A. Put the access keys in Amazon Glacier instead.
B. Put the access keys in an Amazon S3 bucket instead.
C. Remove the stored access keys in the AMI. Create a new IAM role with permissions to access the DynamoDB table and assign it to the EC2 instances.(Correct)
D. Do nothing. The architecture is already secure because the access keys are already in the Amazon Machine Image.

EXPLANATION

You should use an IAM role to manage temporary credentials for applications that run on an EC2 instance. When you use an IAM role, you don't have to distribute long-term credentials (such as a user name and password or access keys) to an EC2 instance.

Instead, the role supplies temporary permissions that applications can use when they make calls to other AWS resources. When you launch an EC2 instance, you specify an IAM role to associate with the instance. Applications that run on the instance can then use the role-supplied temporary credentials to sign API requests.

Hence, the best option here is to remove the stored access keys first in the AMI. Then, create a new IAM role with permissions to access the DynamoDB table and assign it to the EC2 instances.

Options 1 and 2 are because S3 and Glacier are mainly used as a storage option. It is better to use an IAM role instead of storing access keys in these storage services.

Option 4 is because you can make the architecture more secure by using IAM.

Question 9:

You are setting up the required compute resources in your VPC for your application which have workloads that require high, sequential read and write access to very large data sets on local storage. Which of the following instance type is the most suitable one to use in this scenario?

A. Storage Optimized Instances (Correct)
B. Memory Optimized Instances
C. Compute Optimized Instances
D. General Purpose Instances

EXPLANATION

Option 1 is the correct answer. Storage optimized instances are designed for workloads that require high, sequential read and write access to very large data sets on local storage. They are optimized to deliver tens of thousands of low-latency, random I/O operations per second (IOPS) to applications.

Option 2 is because Memory optimized instances are designed to deliver fast performance for workloads that process large data sets in memory, which is quite different from handling high read and write capacity on local storage.

Option 3 is because Compute optimized instances are ideal for compute-bound applications that benefit from high-performance processors, such as batch processing workloads and media transcoding.

Option 4 is because General purpose instances are the most basic type of instances. They provide a balance of compute, memory, and networking resources, and can be used for a variety of workloads. Since you are requiring higher read and write capacity, storage optimized instances should be selected instead.

Question 10:

An application is using a Lambda function to process complex financial data which runs for about 10 to 15 minutes. You noticed that there are a few terminated invocations throughout the day, which caused data discrepancy in the application.

Which of the following is the most likely cause of this issue?

A. **The failed Lambda functions have been running for over 15 minutes and reached the maximum execution time.(Correct)**
B. The concurrent execution limit has been reached.
C. The Lambda function contains a recursive code and has been running for over 15 minutes.
D. The failed Lambda Invocations contain a ServiceException error which means that the AWS Lambda service encountered an internal error.

EXPLANATION

A Lambda function consists of code and any associated dependencies. In addition, a Lambda function also has configuration information associated with it. Initially, you specify the configuration information when you create a Lambda function. Lambda provides an API for you to update some of the configuration data.

You pay for the AWS resources that are used to run your Lambda function. To prevent your Lambda function from running indefinitely, you specify a timeout. When the specified timeout is reached, AWS Lambda terminates execution of your Lambda function. It is recommended that you set this value based on your expected execution time. The default timeout is 3 seconds and the maximum execution duration per request in AWS Lambda is 900 seconds, which is equivalent to 15 minutes. Hence, Option 1 is the correct answer.

Take note that you can invoke a Lambda function synchronously either by calling the Invoke operation or by using an AWS SDK in your preferred runtime. If you anticipate a long-running Lambda function, your client may time out before function execution completes. To avoid this, update the client timeout or your SDK configuration.

Option 2 is because, by default, the AWS Lambda limits the total concurrent executions across all functions within a given region to 1000. By setting a concurrency limit on a function, Lambda guarantees that allocation will be applied specifically to that function, regardless of the amount of traffic processing the remaining functions. If that limit is exceeded, the function will be throttled but not terminated, which is in contrast with what is happening in the scenario.

Option 3 is because having a recursive code in your Lambda function does not directly result to an abrupt termination of the function execution. This is a scenario wherein the function automatically calls itself until some arbitrary criteria is met. This could lead to an unintended volume of function invocations and escalated costs, but not an abrupt termination because Lambda will throttle all invocations to the function.

Option 4 is because although this is a valid root cause, it is unlikely to have several ServiceException errors throughout the day unless there is an outage or disruption in AWS. Since the scenario says that the Lambda function runs for about 10 to 15 minutes, the maximum execution duration is the most likely cause of the issue and not the AWS Lambda service encountering an internal error.

Question 11:

You are trying to enable Cross-Region Replication to your S3 bucket but this option is disabled.

Which of the following options is a valid reason for this?

A. The Cross-Region Replication feature is only available for Amazon S3 - RRS.
B. This is a premium feature which is only for AWS Enterprise accounts.
C. In order to use the Cross-Region Replication feature in S3, you need to first enable versioning on the bucket.(Correct)
D. The Cross-Region Replication feature is only available for Amazon S3 - Infrequent Access.

EXPLANATION

To enable the cross-region replication feature in S3, the following items should be met:

1. The source and destination buckets must have versioning enabled.

2. The source and destination buckets must be in different AWS Regions.

3. Amazon S3 must have permissions to replicate objects from that source bucket to the destination bucket on your behalf.

- Options 1 and 4 are wrong as this feature is available to all types of S3 classes.
- Option 2 is as this CRR feature is available to all Support Plans.

Question 12:

In a tech company that you are working for, there is a requirement to allow one IAM user to modify the configuration of one of your Elastic Load Balancers (ELB). This access is required only once.

Which of the following would be the best way to allow this access?

A. Open up the port that ELB uses in a security group and then give the user access to that security group via a policy.
B. Create a new IAM Role which will be assumed by the IAM user. Attach a policy allowing access to modify the ELB and once it is done, remove the IAM role from the user.(Correct)
C. Create a new IAM user that has access to modify the ELB. Delete that user when the work is completed.
D. Provide the user temporary access to the root account for 8 hours only. Afterwards, change the password once the activity is completed.

EXPLANATION

In this scenario, the best option is to use IAM Role to provide access. You can create a new IAM Role then associate it to the IAM user. Attach a policy allowing access to modify the ELB and once it is done, remove the IAM role to the user.

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

You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources. For example, you might want to grant users in your AWS account access to resources they don't usually have, or grant users in one AWS account access to resources in another account. Or you might want to allow a mobile app to use AWS resources, but not want to embed AWS keys within the app (where they can be difficult to rotate and where users can potentially extract them). Sometimes you want to give AWS access to users who already have identities defined outside of AWS, such as in your corporate directory. Or, you might want to grant access to your account to third parties so that they can perform an audit on your resources.

Question 13:

You have 2 SUSE Linux Enterprise Server instances located in different subnets in the same VPC. These EC2 instances should be able to communicate with each other, but you always get a timeout when you try to ping from one instance to another. In addition, the route tables seem to be valid and have the entry for the Target 'local' for your VPC CIDR.

Which of the following could be a valid reason for this issue?

1. The two EC2 Instances have different versions of the SUSE Linux AMI.
2. **You have not configured the Security Group to allow the required traffic between the two subnets.(Correct)**
3. The EC2 instances do not have Public IPs attached to them.
4. The EC2 Instances do not have Elastic IPs.

EXPLANATION

To ensure that ping commands can go through between EC2 instances, security groups need to be configured. The ping utility uses the ICMP protocol, so this needs to be set in the Inbound Rules of your security group to ensure that the ping packets can be routed to the EC2 instances.

Question 14:

You are instructed by your manager to create a publicly accessible EC2 instance by using an Elastic IP (EIP) address and also to give him a report on how much it will cost to use that EIP.

Which of the following statements is correct regarding the pricing of EIP?

1. **There is no cost if the instance is running and it has only one associated EIP.(Correct)**
2. There is no cost if the instance is terminated and it has only one associated EIP.
3. There is no cost if the instance is stopped and it has only one associated EIP.
4. There is no cost if the instance is running and it has at least two associated EIP.

EXPLANATION

An Elastic IP address doesn’t incur charges as long as the following conditions are true:

- -The Elastic IP address is associated with an Amazon EC2 instance.
- -The instance associated with the Elastic IP address is running.
- -The instance has only one Elastic IP address attached to it.

If you’ve stopped or terminated an EC2 instance with an associated Elastic IP address and you don’t need that Elastic IP address anymore, consider disassociating or releasing the Elastic IP address .

Question 15:

A web application, which is hosted in your on-premises data center and uses a MySQL database, must be migrated to AWS Cloud. You need to ensure that the network traffic to and from your RDS database instance is encrypted using SSL. For improved security, you have to use the profile credentials specific to your EC2 instance to access your database, instead of a password.

Which of the following should you do to meet the above requirement?

A. Launch a new RDS database instance with the Backtrack feature enabled.
B. Configure your RDS database to enable encryption.
C. Set up an RDS database and enable the IAM DB Authentication.(Correct)
D. Launch the mysql client using the --ssl-ca parameter when connecting to the database.

EXPLANATION

You can authenticate to your DB instance using AWS Identity and Access Management (IAM) database authentication. IAM database authentication works with MySQL and PostgreSQL. With this authentication method, you don't need to use a password when you connect to a DB instance. Instead, you use an authentication token.

An authentication token is a unique string of characters that Amazon RDS generates on request. Authentication tokens are generated using AWS Signature Version 4. Each token has a lifetime of 15 minutes. You don't need to store user credentials in the database, because authentication is managed externally using IAM. You can also still use standard database authentication.

IAM database authentication provides the following benefits:

- Network traffic to and from the database is encrypted using Secure Sockets Layer (SSL).
- You can use IAM to centrally manage access to your database resources, instead of managing access individually on each DB instance.
- For applications running on Amazon EC2, you can use profile credentials specific to your EC2 instance to access your database instead of a password, for greater security

Hence, Option 3 is the correct answer based on the above reference.

Option 1 is because the Backtrack feature simply "rewinds" the DB cluster to the time you specify. Backtracking is not a replacement for backing up your DB cluster so that you can restore it to a point in time. However, you can easily undo mistakes using the backtrack feature if you mistakenly perform a destructive action, such as a DELETE without a WHERE clause.

Option 2 is because the encryption feature in RDS is mainly for securing your Amazon RDS DB instances and snapshots at rest. The data that is encrypted at rest includes the underlying storage for DB instances, its automated backups, Read Replicas, and snapshots.

Option 4 is because even though using the --ssl-ca parameter can provide SSL connection to your database, you still need to use IAM database connection to use the profile credentials specific to your EC2 instance to access your database instead of a password.

Question 16:

A startup company wants to launch a fleet of EC2 instances on AWS. Your manager wants to ensure that the Java programming language is installed automatically when the instance is launched. In which of the below configurations can you achieve this requirement?

A. **User data(Correct)**
B. EC2Config service
C. IAM roles
D. AWS Config

EXPLANATION

When you launch an instance in Amazon EC2, you have the option of passing user data to the instance that can be used to perform common automated configuration tasks and even run scripts after the instance starts. You can write and run scripts that install new packages, software, or tools in your instance when it is launched.

You can pass two types of user data to Amazon EC2: shell scripts and cloud-init directives. You can also pass this data into the launch wizard as plain text, as a file (this is useful for launching instances using the command line tools), or as base64-encoded text (for API calls).

Question 17:

You are working as a Solutions Architect for a major accounting firm, and they have a legacy general ledger accounting application that needs to be moved to AWS. However, the legacy application has a dependency on multicast networking. On this scenario, which of the following options should you consider to ensure the legacy application works in AWS?

A. Provision Elastic Network Interfaces between the subnets.
B. Create all the subnets on another VPC and enable VPC peering.
C. Create a virtual overlay network running on the OS level of the instance.(Correct)
D. All of the above.

EXPLANATION

Multicast is a network capability that allows one-to-many distribution of data. With multicasting, one or more sources can transmit network packets to subscribers that typically reside within a multicast group. However, take note that Amazon VPC does not support multicast or broadcast networking.

You can use an overlay multicast in order to migrate the legacy application. An overlay multicast is a method of building IP level multicast across a network fabric supporting unicast IP routing, such as Amazon Virtual Private Cloud (Amazon VPC).

Option 1 is because just providing ENIs between the subnets would not resolve the dependency on multicast.

Option 2 is because VPC peering and multicast are not the same.

Option 3 is correct because overlay multicast is a method of building IP level multicast across a network fabric supporting unicast IP routing, such as Amazon Virtual Private Cloud (Amazon VPC).

Option 4 is because the only option that will work in this scenario is creating a virtual overlay network.

Question 18:

A multinational manufacturing company has multiple accounts in AWS to separate their various departments such as finance, human resources, engineering and many others. There is a requirement to ensure that certain

access to services and actions are properly controlled to comply with the security policy of the company.

As the Solutions Architect, which is the most suitable way to set up the multi-account AWS environment of the company?

A. Set up a common IAM policy that can be applied across all AWS accounts.
B. Connect all departments by setting up a cross-account access to each of the AWS accounts of the company. Create and attach IAM policies to your resources based on their respective departments to control access.
C. Provide access to externally authenticated users via Identity Federation. Set up an IAM role to specify permissions for users from each department whose identity is federated from your organization or a third-party identity provider.
D. Use AWS Organizations and Service Control Policies to control services on each account.(Correct)

EXPLANATION

Option 4 is the correct answer. Refer to the diagram below:

AWS Organizations offers policy-based management for multiple AWS accounts. With Organizations, you can create groups of accounts, automate account creation, apply and manage policies for those groups. Organizations enables you to centrally manage policies across multiple accounts, without requiring custom scripts and manual processes. It allows you to create Service Control Policies (SCPs) that centrally control AWS service use across multiple AWS accounts.

Option 1 is because it is not possible to create a common IAM policy for multiple AWS accounts.

Option 2 is because although you can set up cross-account access to each department, this entails a lot of configuration compared with using AWS Organizations and Service Control Policies (SCPs). Cross-account access would be a more suitable choice if you only have two accounts to manage, but not for multiple accounts.

Option 3 is as this option is focused on the Identity Federation authentication set up for your AWS accounts but not the IAM policy management for multiple AWS accounts. A combination of AWS Organizations and Service Control Policies (SCPs) is a better choice compared to this option.

Question 19:

You are working for a global news network where you have set up a CloudFront distribution for your web application. However, you noticed that your application's origin server is being hit for each request instead of the AWS Edge locations, which serve the cached objects. The issue occurs even for the commonly requested objects.

What could be a possible cause of this issue?

A. An object is only cached by Cloudfront once a successful request has been made hence, the objects were not requested before, which is why the request is still directed to the origin server.
B. The file sizes of the cached objects are too large for CloudFront to handle.
C. The Cache-Control max-age directive is set to zero.(Correct)
D. You did not add an SSL certificate.

EXPLANATION

In this scenario, the main culprit is that the Cache-Control max-age directive is set to a low value, which is why the request is always directed to your origin server. Hence, option 3 is correct.

Option 1 is because the issue also occurs even for the commonly requested objects. This means that these objects were successfully requested before but due to a low Cache-Control max-age directive value, it causes this issue in Cloudfront.

Options 2 and 4 are because they are not related to the issue in caching.

You can control how long your objects stay in a CloudFront cache before CloudFront forwards another request to your origin. Reducing the duration allows you to serve dynamic content. Increasing the duration means your users get better performance because your objects are more likely to be served directly from the edge cache. A longer duration also reduces the load on your origin.

Typically, CloudFront serves an object from an edge location until the cache duration that you specified passes — that is, until the object expires. After it expires, the next time the edge location gets a user request for the object, CloudFront forwards the request to the origin server to verify that the cache contains the latest version of the object.

The Cache-Control and Expires headers control how long objects stay in the cache. The Cache-Control max-age directive lets you specify how long (in seconds) you want an object to remain in the cache before CloudFront gets the object again from the origin server. The minimum expiration time CloudFront supports is 0 seconds for web distributions and 3600 seconds for RTMP distributions.

Question 20:

AWS hosts a variety of public datasets such as satellite imagery, geospatial, or genomic data that you want to use for your web application hosted in Amazon EC2.

If you use these datasets, how much will it cost you?

A. A one-time charge of $10.
B. $10 per month for each dataset.

C. $10 per month for all datasets.
D. No charge.(Correct)

EXPLANATION

AWS hosts a variety of public datasets that anyone can access for free.

Previously, large datasets such as satellite imagery or genomic data have required hours or days to locate, download, customize, and analyze. When data is made publicly available on AWS, anyone can analyze any volume of data without needing to download or store it themselves.

Question 21:

A game development company operates several virtual reality (VR) and augmented reality (AR) games which use various RESTful web APIs hosted on their on-premises data center. Due to the unprecedented growth of their company, they decided to migrate their system to AWS Cloud to scale out their resources as well to minimize costs.

Which of the following should you recommend as the most cost-effective and scalable solution to meet the above requirement?

A. Use AWS Lambda and Amazon API Gateway.(Correct)
B. Set up a micro-service architecture with ECS, ECR, and Fargate.
C. Host the APIs in a static S3 web hosting bucket behind a CloudFront web distribution.
D. Use Spot Amazon EC2 instances behind an Application Load Balancer.

EXPLANATION

With AWS Lambda, you pay only for what you use. You are charged based on the number of requests for your functions and the duration, the time it takes for your code to execute.

Lambda counts a request each time it starts executing in response to an event notification or invoke call, including test invokes from the console. You are charged for the total number of requests across all your functions. Duration is calculated from the time your code begins executing until it returns or otherwise terminates, rounded up to the nearest 100ms. The price depends on the amount of memory you allocate to your function. The Lambda free tier includes 1M free requests per month and over 400,000 GB-seconds of compute time per month.

The best possible answer here is to use Lambda and API Gateway because this solution is both scalable and cost-effective. You will only be charged when you use your Lambda function, unlike having an EC2 instance which always runs even though you don’t use it.

Option 2 is because ECS is mainly used to host Docker applications and in addition, using ECS, ECR, and Fargate alone is not scalable and not recommended for this type of scenarios.

Option 3 is not a suitable option as there is no compute capability for S3 and you can only use it as a static website. Although this solution is scalable since it is using CloudFront, the use of S3 to host the web APIs or the dynamic website is still .

Option 4 is because EC2 alone, without Auto Scaling, is not scalable. Even though you use Spot EC2 instance, it is still more expensive compared to Lambda because you will be charged only when your function is being used.

Question 22:

You are working as a Cloud Engineer in a leading technology consulting firm which is using a fleet of Windows-based EC2 instances with IPv4 addresses launched in a private subnet. Several software installed in the EC2 instances are required to be updated via the Internet.

Which of the following services can provide you with a highly available solution to safely allow the instances to fetch the software patches from the Internet but prevent outside network from initiating a connection?

A. Egress-Only Internet Gateway
B. VPC Endpoint
C. NAT Gateway(Correct)
D. NAT Instance

EXPLANATION

AWS offers two kinds of NAT devices — a NAT gateway or a NAT instance. It is recommended to use NAT gateways, as they provide better availability and bandwidth over NAT instances. The NAT Gateway service is also a managed service that does not require your administration efforts. A NAT instance is launched from a NAT AMI.

Just like a NAT instance, you can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances.

Here is a diagram showing the differences between NAT gateway and NAT instance:

Option 1 is because an Egress-only Internet gateway is primarily used for VPCs that use IPv6 to enable instances in a private subnet to connect to the Internet or other AWS services, but prevent the Internet from initiating a connection with those instances, just like what NAT Instance and NAT Gateway do. The scenario explicitly says that the EC2 instances are using IPv4 addresses which is why Egress-only Internet gateway is invalid, even though it can provide the required high availability.

Option 2 is because a VPC endpoint simply 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.

Option 4 is because although a NAT instance can also enable instances in a private subnet to connect to the Internet or other AWS services and prevent the Internet from initiating a connection with those instances, it is not as highly available compared to a NAT Gateway.

Question 23:

Your company has developed a financial analytics web application hosted in a Docker container using MEAN (MongoDB, Express.js, AngularJS, and Node.js) stack. You want to easily port that web application to AWS Cloud which can automatically handle all the tasks such as balancing load, auto-scaling, monitoring, and placing your containers across your cluster.

Which of the following services can be used to fulfill this requirement?

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

EXPLANATION

Elastic Beanstalk supports the deployment of web applications from Docker containers. With Docker containers, you can define your own runtime environment. You can choose your own platform, programming language, and any application dependencies (such as package managers or tools), that aren't supported by other platforms. Docker containers are self-contained and include all the configuration information and software your web application requires to run.

By using Docker with Elastic Beanstalk, you have an infrastructure that automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring. You can manage your web application in an environment that supports the range of services that are integrated with Elastic Beanstalk, including but not limited to VPC, RDS, and IAM. Hence, Option 4 is correct.

Option 1 is because although ECS also provides Service Auto Scaling, Service Load Balancing and Monitoring with CloudWatch, these features are not automatically enabled by default unlike with Elastic Beanstalk. Take note that the scenario requires a service that will automatically handle all the tasks such as balancing load, auto-scaling, monitoring, and placing your containers across your cluster. You will have to manually configure these things if you wish to use ECS. With Elastic Beanstalk, you can manage your web application in an environment that supports the range of services easier.

Options 2 and 3 are because OpsWorks and CodeDeploy are primarily used for application deployment and configuration only, without providing load balancing, auto-scaling, monitoring or ECS cluster management.

Question 24:

You are working for a computer animation film studio that has a web application running on an Amazon EC2 instance. It uploads 5 GB video objects to an Amazon S3 bucket. Video uploads are taking longer than expected, which impacts the performance of your application.

Which method will help improve the performance of your application?

A. Enable Enhanced Networking to your EC2 Instances.
B. Use Amazon S3 Multipart Upload API.(Correct)
C. Leverage on Amazon CloudFront and use HTTP POST method to reduce latency.
D. Use Amazon Elastic Block Store Provisioned IOPS and an Amazon EBS-optimized instance.

EXPLANATION

The main issue is the slow upload time of the video objects to Amazon S3. To address this issue, you can use Multipart upload in S3 to improve the throughput. It allows you to upload parts of your object in parallel thus, decreasing the time it takes to upload big objects. Each part is a contiguous portion of the object's data.

You can upload these object parts independently and in any order. If transmission of any part fails, you can retransmit that part without affecting other parts. After all parts of your object are uploaded, Amazon S3 assembles these parts and creates the object. In general, when your object size reaches 100 MB, you should consider using multipart uploads instead of uploading the object in a single operation.

Using multipart upload provides the following advantages:

1. Improved throughput - You can upload parts in parallel to improve throughput.

2. Quick recovery from any network issues - Smaller part size minimizes the impact of restarting a failed upload due to a network error.

3. Pause and resume object uploads - You can upload object parts over time. Once you initiate a multipart upload, there is no expiry; you must explicitly complete or abort the multipart upload.

4. Begin an upload before you know the final object size - You can upload an object as you are creating it.

Question 25:

A mobile application stores pictures in Amazon Simple Storage Service (S3) and allows application sign-in using an OpenID Connect-compatible identity provider.

Which AWS Security Token Service approach to temporary access should you use for this scenario?

A. SAML-based Identity Federation
B. Cross-Account Access
C. AWS Identity and Access Management roles
D. Web Identity Federation(Correct)

EXPLANATION

With web identity federation, you don't need to create custom sign-in code or manage your own user identities. Instead, users of your app can sign in using a well-known identity provider (IdP) —such as Login with Amazon, Facebook, Google, or any other OpenID Connect (OIDC)-compatible IdP, receive an authentication token, and then exchange that token for temporary security credentials in AWS that map to an IAM role with permissions to use the resources in your AWS account. Using an IdP helps you keep your AWS account secure because you don't have to embed and distribute long-term security credentials with your application.

Question 26:

As the Solutions Architect, you have built a photo-sharing site for an entertainment company. The site was hosted using 3 EC2 instances in a single availability zone with a Classic Load Balancer in front to evenly distribute the incoming load.

What should you do to enable your Classic Load Balancer to bind a user's session to a specific instance?

A. Sticky Sessions(Correct)
B. Availability Zone
C. Placement Group
D. Security Group

EXPLANATION

By default, a Classic Load Balancer routes each request independently to the registered instance with the smallest load. However, you can use the sticky session feature (also known as session affinity), which enables the load balancer to bind a user's session to a specific instance. This ensures that all requests from the user during the session are sent to the same instance.

The key to managing sticky sessions is to determine how long your load balancer should consistently route the user's request to the same instance. If your application has its own session cookie, then you can configure Elastic Load Balancing so that the session cookie follows the duration specified. If your application does not have its own session cookie, then you can configure Elastic Load Balancing to create a session cookie by specifying your own stickiness duration.

Question 27:

A multinational company has been building its new generation big data and analytics platform in AWS in which they need a scalable storage service. The data need to be stored redundantly across multiple AZ's and allows concurrent connections from multiple EC2 instances hosted on multiple Availability Zones.

Which of the following AWS storage service is the best one to use in this scenario?

A. EBS Volumes
B. Elastic File System(Correct)
C. Amazon S3
D. ElastiCache

EXPLANATION

In this question, you should take note of this phrase: "allows concurrent connections from multiple EC2 instances". There are various AWS storage options that you can choose but whenever these criteria show up, always consider using EFS instead of using EBS Volumes which is mainly used as a "block" storage and can only have one connection to one EC2 instance at a time.

Amazon EFS is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud. With a few clicks in the AWS Management Console, you can create file systems that are accessible to Amazon EC2 instances via a file system interface (using standard operating system file I/O APIs) and supports full file system access semantics (such as strong consistency and file locking).

Amazon EFS file systems can automatically scale from gigabytes to petabytes of data without needing to provision storage. Tens, hundreds, or even thousands of Amazon EC2 instances can access an Amazon EFS file system at the same time, and Amazon EFS provides consistent performance to each Amazon EC2 instance. Amazon EFS is designed to be highly durable and highly available.

Question 28:

You are a Solutions Architect of a tech company. You are having an issue whenever you try to connect to your newly created EC2 instance using a Remote Desktop connection from your computer. Upon checking, you have

verified that the instance has a public IP and the Internet gateway and route tables are in place.

What else should you do for you to resolve this issue?

A. You should adjust the security group to allow traffic from port 22
B. You should adjust the security group to allow traffic from port 3389(Correct)
C. You should restart the EC2 instance since there might be some issue with the instance
D. You should create a new instance since there might be some issue with the instance

EXPLANATION

Since you are using a Remote Desktop connection to access your EC2 instance, you have to ensure that the Remote Desktop Protocol is allowed in the security group. By default, the server listens on TCP port 3389 and UDP port 3389.

Option 1 is as the port 22 is used for SSH connections and not for RDP.

Options 3 and 4 are as the EC2 instance is newly created and hence, unlikely to cause the issue. You have to check the security group first if it allows the Remote Desktop Protocol (3389) before investigating if there is indeed an issue on the specific instance.

Question 29:

You were hired as an IT Consultant in a startup cryptocurrency company that wants to go global with their international money transfer app. Your project is to make sure that the database of the app is highly available on multiple regions.

What are the benefits of adding Multi-AZ deployments in Amazon RDS?

A. It makes the database fault-tolerant to an Availability Zone failure.(Correct)
B. Significantly increases the database performance.
C. Creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ) in a different region.
D. Increased database availability in the case of system upgrades like OS patching or DB Instance scaling.(Correct)
E. Provides SQL optimization.

EXPLANATION

The correct answers are options 1 & 4:

- Increased database availability in the case of system upgrades like OS patching or DB Instance scaling.

- It makes the database fault-tolerant to an Availability Zone failure

Option 3 is almost correct. RDS synchronously replicates the data to a standby instance in a different Availability Zone (AZ) that is in the same region and not in a different one.

Options 2 and 5 are as it does not affect the performance nor provide SQL optimization.

Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable.

In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby (or to a read replica in the case of Amazon Aurora), so that you can resume database operations as soon as the failover is complete. Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention.

Question 30:

You are building a microservices architecture in which a software is composed of small independent services that communicate over well-defined APIs. In building large-scale systems, fine-grained decoupling of microservices is a recommended practice to implement. The decoupled services should scale horizontally from each other to improve scalability.

What is the difference between Horizontal scaling and Vertical scaling?

A. Vertical scaling means running the same software on a fully serverless architecture using Lambda. Horizontal scaling means adding more servers to the existing pool and it doesn’t run into limitations of individual servers.
B. Horizontal scaling means running the same software on bigger machines which is limited by the capacity of individual servers. Vertical scaling is adding more servers to the existing pool and doesn’t run into limitations of individual servers.
C. Vertical scaling means running the same software on bigger machines which is limited by the capacity of the individual server. Horizontal scaling is adding more servers to the existing pool and doesn’t run into limitations of individual servers.(Correct)
D. Horizontal scaling means running the same software on smaller containers such as Docker and Kubernetes using ECS or EKS. Vertical scaling is adding more servers to the existing pool and doesn’t run into limitations of individual servers.

EXPLANATION

Vertical scaling means running the same software on bigger machines which is limited by the capacity of the individual server. Horizontal scaling is adding more servers to the existing pool and doesn’t run into limitations of individual servers.

Fine-grained decoupling of microservices is a best practice for building large-scale systems. It’s a prerequisite for performance optimization since it allows choosing the appropriate and optimal technologies for a specific service. Each service can be implemented with the appropriate programming languages and frameworks, leverage the optimal data persistence solution, and be fine-tuned with the best performing service configurations.

Properly decoupled services can be scaled horizontally and independently from each other. Vertical scaling, which is running the same software on bigger machines, is limited by the capacity of individual servers and can incur downtime during the scaling process. Horizontal scaling, which is adding more servers to the existing pool, is highly dynamic and doesn’t run into limitations of individual servers. The scaling process can be completely automated.

Furthermore, the resiliency of the application can be improved because failing components can be easily and automatically replaced. Hence, Option 3 is the correct answer.

Option 1 is because Vertical scaling is not about running the same software on a fully serverless architecture. AWS Lambda is not required for scaling.

Option 2 is because the definitions for the two concepts were switched. Vertical scaling means running the same software on bigger machines which is limited by the capacity of the individual server. Horizontal scaling is adding more servers to the existing pool and doesn’t run into limitations of individual servers.

Option 4 is because Horizontal scaling is not related to using ECS or EKS containers on a smaller instance.

Question 31:

You have created a VPC with a single subnet then you launched an On-Demand EC2 instance in that subnet. You have attached Internet gateway (IGW) to the VPC and verified that the EC2 instance has a public IP. The main route table of the VPC is as shown below:

However, the instance still cannot be reached from the Internet when you tried to connect to it from your computer. Which of the following should be made to the route table to fix this issue?

A. Add this new entry to the route table: 0.0.0.0/27 -> Your Internet Gateway
B. Modify the above route table: 10.0.0.0/27 -> Your Internet Gateway
C. Add the following entry to the route table: 10.0.0.0/27 -> Your Internet Gateway
D. Add a new entry to the route table - 0.0.0.0/27 -> Internet Gateway

E. **Add this new entry to the route table: 0.0.0.0/0 -> Your Internet Gateway(Correct)**

EXPLANATION

Apparently, the route table does not have an entry for the Internet Gateway. This is why you cannot connect to the EC2 instance. To fix this, you have to add a route with a destination of 0.0.0.0/0 for IPv4 traffic or ::/0 for IPv6 traffic, and then a target of the Internet gateway ID (igw-xxxxxxxx).

This should be the correct route table configuration after adding the new entry.

Question 32:

The company that you are working for has instructed you to create a cost-effective cloud solution for their online movie ticketing service. Your team has designed a solution of using a fleet of Spot EC2 instances to host the new ticketing web application. You requested a spot instance at a maximum price of $0.06/hr which has been fulfilled immediately. After 45 minutes, the spot price increased to $0.08/hr and then your instance was terminated by AWS.

What was the total EC2 compute cost of running your spot instances?

A. **$0.00(Correct)**
B. $0.06
C. $0.08
D. $0.07

EXPLANATION

In this scenario, you don't need to pay at all hence, option 1 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 33:

A global medical research company has a molecular imaging system which provides each client with frequently updated images of what is happening inside the human body at the molecular and cellular level. The system is hosted in AWS and the images are hosted in an S3 bucket behind a CloudFront web distribution. There was a new batch of updated images that

were uploaded in S3, however, the users were reporting that they were still seeing the old content. You need to control which image will be returned by the system even when the user has another version cached either locally or behind a corporate caching proxy.

Which of the following is the most suitable solution to solve this issue?

A. **Use versioned objects(Correct)**
B. Invalidate the files in your CloudFront web distribution
C. Add a separate cache behavior path for the content and configure a custom object caching with a Minimum TTL of 0
D. Add Cache-Control no-cache, no-store, or private directives to the objects that you don't want CloudFront to cache.

EXPLANATION

To control the versions of files that are served from your distribution, you can either invalidate files or give them versioned file names. If you want to update your files frequently, AWS recommends that you primarily use file versioning for the following reasons:

- -Versioning enables you to control which file a request returns even when the user has a version cached either locally or behind a corporate caching proxy. If you invalidate the file, the user might continue to see the old version until it expires from those caches.

- -CloudFront access logs include the names of your files, so versioning makes it easier to analyze the results of file changes.

- -Versioning provides a way to serve different versions of files to different users.

- -Versioning simplifies rolling forward and back between file revisions.

- -Versioning is less expensive. You still have to pay for CloudFront to transfer new versions of your files to edge locations, but you don't have to pay for invalidating files.

Option 2 is because even though using invalidation will solve this issue, this solution is more expensive as compared to Option 1.

Option 3 is because configuring a separate cache behavior path having a custom object caching with a Minimum TTL of 0 alone is not enough to solve the problem. A cache behavior is primarily used to configure a variety of CloudFront functionality for a given URL path pattern for files on your website. Although this solution may work, it is still better to use versioned objects where you can control which image will be returned by the system even when the user has another version cached either locally or behind a corporate caching proxy.

Option 4 is because although it is right to configure your origin to add the Cache-Control or Expires header field, you should do this to your objects and not on the entire S3 bucket.

Question 34:

Your company would like to store their old yet confidential corporate files that are infrequently accessed. What cost-efficient solution in AWS should you recommend?

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

EXPLANATION

Amazon Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup. It is designed to deliver 99.999999999% durability, and provides comprehensive security and compliance capabilities that can help meet even the most stringent regulatory requirements. Amazon Glacier provides query-in-place functionality, allowing you to run powerful analytics directly on your archive data at rest.

Question 35:

You are planning to launch an application that tracks the GPS coordinates of delivery trucks in your country. The coordinates are transmitted from each delivery truck every five seconds. You need to design an architecture that will enable real-time processing of these coordinates from multiple consumers. The aggregated data will be analyzed in a separate reporting application.

Which AWS service should you use for this scenario?

A. Amazon Kinesis(Correct)
B. AWS Data Pipeline
C. Amazon AppStream
D. Amazon Simple Queue Service

EXPLANATION

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. It 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 responds instantly instead of having to wait until all your data are collected before the processing can begin.

Question 36:

You are working as an AWS Engineer in a major telecommunications company in which you are tasked to make a network monitoring system. You launched an EC2 instance to host the monitoring system and used CloudWatch to monitor, store, and access the log files of your instance.

Which of the following provides an automated way to send log data to CloudWatch Logs from your Amazon EC2 instance?

A. **CloudWatch Logs agent(Correct)**
B. CloudTrail
C. VPC Flow Logs
D. CloudTrail Logs agent

EXPLANATION

CloudWatch Logs agent provides an automated way to send log data to CloudWatch Logs from Amazon EC2 instances hence, Option 1 is the correct answer.

The CloudWatch Logs agent is comprised of the following components:

- -A plug-in to the AWS CLI that pushes log data to CloudWatch Logs.
- -A script (daemon) that initiates the process to push data to CloudWatch Logs.
- -A cron job that ensures that the daemon is always running.

Option 2 is as CloudTrail is mainly used for tracking the API calls of your AWS resources and not for sending EC2 logs to CloudWatch.

Option 3 is as VPC Flow logs is mainly used for tracking the traffic coming into the VPC and not for EC2 instance monitoring.

Option 4 is because CloudTrail Logs agent does not exist.

Question 37:

A web application is hosted on a fleet of EC2 instances inside an Auto Scaling Group with a couple of Lambda functions for ad hoc processing. Whenever

you release updates to your application every week, there are inconsistencies where some resources are not updated properly. You need a way to group the resources together and deploy the new version of your code consistently among the groups with minimal downtime.

Which among these options should you do to satisfy the given requirement with the least effort?

A. Create CloudFormation templates that have the latest configurations and code in them.
B. Use CodeCommit to publish your code quickly in a private repository and push them to your resources for fast updates.
C. Use deployment groups in CodeDeploy to automate code deployments in a consistent manner.(Correct)
D. Create OpsWorks recipes that will automatically launch resources containing the latest version of the code.

EXPLANATION

CodeDeploy is a deployment service that automates application deployments to Amazon EC2 instances, on-premises instances, or serverless Lambda functions. It allows you to rapidly release new features, update Lambda function versions, avoid downtime during application deployment, and handle the complexity of updating your applications, without many of the risks associated with error-prone manual deployments.

Option 1 is since it is used for provisioning and managing stacks of AWS resources based on templates you create to model your infrastructure architecture. CloudFormation is recommended if you want a tool for granular control over the provisioning and management of your own infrastructure.

Option 2 is as you mainly use CodeCommit for managing a source-control service that hosts private Git repositories. You can store anything from code to binaries and work seamlessly with your existing Git-based tools. CodeCommit integrates with CodePipeline and CodeDeploy to streamline your development and release process.

You could also use OpsWorks to deploy your code, however, option 4 is still because you don't need to launch new resources containing your new code when you can just update the ones that are already running.

Question 38:

An online shopping platform has been deployed to AWS using Elastic Beanstalk. They simply uploaded their Node.js application, and Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring. Since the entire deployment process is automated, the DevOps team is not sure where to get the application log files of their shopping platform.

In Elastic Beanstalk, where does it store the application files and server log files?

A. Application files are stored in S3. The server log files can only be stored in the attached EBS volumes of the EC2 instances, which were launched by AWS Elastic Beanstalk.
B. Application files are stored in S3. The server log files can be stored directly in Glacier or in CloudWatch Logs.
C. Application files are stored in S3. The server log files can be optionally stored in CloudTrail or in CloudWatch Logs.
D. Application files are stored in S3. The server log files can also optionally be stored in S3 or in CloudWatch Logs. (Correct)

EXPLANATION

Option 4 is correct. AWS Elastic Beanstalk stores your application files and optionally, server log files in Amazon S3. If you are using the AWS Management Console, the AWS Toolkit for Visual Studio, or AWS Toolkit for Eclipse, an Amazon S3 bucket will be created in your account and the files you upload will be automatically copied from your local client to Amazon S3. Optionally, you may configure Elastic Beanstalk to copy your server log files every hour to Amazon S3. You do this by editing the environment configuration settings.

With CloudWatch Logs, you can monitor and archive your Elastic Beanstalk application, system, and custom log files from Amazon EC2 instances of your environments. You can also configure alarms that make it easier for you to react to specific log stream events that your metric filters extract. The CloudWatch Logs agent installed on each Amazon EC2 instance in your environment publishes metric data points to the CloudWatch service for each log group you configure. Each log group applies its own filter patterns to determine what log stream events to send to CloudWatch as data points. Log streams that belong to the same log group share the same retention, monitoring, and access control settings. You can configure Elastic Beanstalk to automatically stream logs to the CloudWatch service.

Option 1 is because the server log files can also be stored in either S3 or CloudWatch Logs, and not only on the EBS volumes of the EC2 instances which are launched by AWS Elastic Beanstalk.

Option 2 is because the server log files can optionally be stored in either S3 or CloudWatch Logs, but not directly to Glacier. You can create a lifecycle policy to the S3 bucket to store the server logs and archive it in Glacier, but there is no direct way of storing the server logs to Glacier using Elastic Beanstalk unless you do it programmatically.

Option 3 is because the server log files can optionally be stored in either S3 or CloudWatch Logs, but not directly to CloudTrail as this service is primarily used for auditing API calls.

Question 39:

You are working as a Solutions Architect in a global investment bank which requires corporate IT governance and cost oversight of all of their AWS resources across their divisions around the world. Their corporate divisions want to maintain administrative control of the discrete AWS resources they consume and ensure that those resources are separate from other divisions.

Which of the following options will support the autonomy of each corporate division while enabling the corporate IT to maintain governance and cost oversight?

A. Use AWS Trusted Advisor
B. Enable IAM cross-account access for all corporate IT administrators in each child account.(Correct)
C. Create separate VPCs for each division within the corporate IT AWS account.
D. Use AWS Consolidated Billing by creating AWS Organizations to link the divisions' accounts to a parent corporate account.(Correct)
E. Create separate Availability Zones for each division within the corporate IT AWS account.

EXPLANATION

In this scenario, Options 2 and 4 are the correct choices. The combined use of IAM and Consolidated Billing will support the autonomy of each corporate division while enabling corporate IT to maintain governance and cost oversight.

You can use an IAM role to delegate access to resources that are in different AWS accounts that you own. You share resources in one account with users in a different account. By setting up cross-account access in this way, you don't need to create individual IAM users in each account. In addition, users don't have to sign out of one account and sign into another in order to access resources that are in different AWS accounts.

You can use the consolidated billing feature in AWS Organizations to consolidate payment for multiple AWS accounts or multiple AISPL accounts. With consolidated billing, you can see a combined view of AWS charges incurred by all of your accounts. You can also get a cost report for each member account that is associated with your master account. Consolidated billing is offered at no additional charge. AWS and AISPL accounts can't be consolidated together.

Option 1 is . Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices. It only provides you alerts on areas where you do not adhere to best practices and tells you how to improve them. It does not assist in maintaining governance over your AWS accounts.

Option 3 is because creating separate VPCs would not separate the divisions from each other since they will still be operating under the same account and therefore contribute to the same billing each month.

Option 5 is because you do not need to create Availability Zones. They are already provided for you by AWS right from the start, and not all services support multiple AZ deployments. In addition, having separate Availability Zones in your VPC does not meet the requirement of supporting the autonomy of each corporate division.

Question 40:

A well-known liquor company has a legacy application which needs to be transferred to the AWS cloud. The legacy application has a dependency on the license which is based on its media access control (MAC) address. They will launch the application in an on-demand EC2 instance. The company has hired you to assist them in this transition.

In this scenario, what can you do to ensure that the MAC address of the EC2 instance will not change even if the instance is restarted or rebooted?

A. Create a VPC with a public and private subnet. The public subnet will house the EC2 instances, while the private subnet will house the dependent license.
B. Ensure EC2 instances that you deploy have their static IP addresses mapped to the MAC address.
C. Provision an ENI with a fixed MAC address.(Correct)
D. Create a VPC with the MAC address tied to its private subnet.

EXPLANATION

An elastic network interface (ENI) is a logical networking component in a VPC that represents a virtual network card. A network interface can include the following attributes: a primary private IPv4 address from the IPv4 address range of your VPC, One or more secondary private IPv4 addresses from the IPv4 address range of your VPC; one Elastic IP address (IPv4) per private IPv4 address; one public IPv4 address; one or more IPv6 addresses; one or more security groups; MAC address and many other network interfaces.

Option 1 is because putting license server in private subnet would not resolve the dependency on the license that is based on a MAC address.

Option 2 is because you cannot map a static IP address to a MAC address.

Option 3 is correct because you should use Elastic Network Interface that is associated with a fixed MAC address. This will ensure that the legacy license based software would always work and not lose the MAC address at any point in the future.

Option 4 is because MAC addresses cannot be tied to subnets.

Question 41:

You are working as a Senior Solutions Architect for a data analytics company which has a VPC for their human resource department, and another VPC for their finance department. You need to configure your architecture to allow the finance department to access all resources that are in the human resource department and vice versa.

Which type of networking connection in AWS should you set up to satisfy the above requirement?

A. VPC Connection
B. VPN Connection
C. VPC Endpoint
D. VPC Peering(Correct)

EXPLANATION

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region.

AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.

Option 1 is since a VPC connection is rather a broad term which encompasses all connections to your VPC. In this scenario, the most suitable connection type to establish is a VPC peering connection.

Option 2 is because a VPN connection does not let you share the resources of each VPC with each other. It only creates a network connection between the two VPCs.

Option 3 is because a VPC Endpoint is primarily used to allow you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink, but not to the other VPC itself.

Question 42:

A top university has recently launched its online learning portal where the students can take e-learning courses from the comforts of their homes. The portal is on a large On-Demand EC2 instance with a single Amazon Aurora database.

How can you improve the availability of your Aurora database to prevent any unnecessary downtime of the online portal?

A. **Create Amazon Aurora Replicas.(Correct)**
B. Deploy Aurora to two Auto-Scaling groups of EC2 instances across two Availability Zones with an elastic load balancer which handles load balancing.
C. Enable Hash Joins to improve the database query performance.
D. Use an Asynchronous Key Prefetch in Amazon Aurora to improve the performance of queries that join tables across indexes.

EXPLANATION

Amazon Aurora MySQL and Amazon Aurora PostgreSQL support Amazon Aurora Replicas, which share the same underlying volume as the primary instance. Updates made by the primary are visible to all Amazon Aurora Replicas. With Amazon Aurora MySQL, you can also create MySQL Read Replicas based on MySQL's binlog-based replication engine. In MySQL Read Replicas, data from your primary instance is replayed on your replica as transactions. For most use cases, including read scaling and high availability, we recommend using Amazon Aurora Replicas.

Hence, the right answer here is Option 1.

Option 2 is because Aurora is a database engine for RDS and not deployed on a typical EC2 instance.

Option 3 is because Hash Joins are mainly used if you need to join a large amount of data by using an equijoin and not for improving availability.

Option 4 is because the Asynchronous Key Prefetch is mainly used to improve the performance of queries that join tables across indexes.

Question 43:

A commercial bank has designed their next generation online banking platform to use a distributed system architecture. As their Software Architect, you have to ensure that their architecture is highly scalable, yet still cost-effective. Which of the following will provide the most suitable solution for this scenario?

A. Launch multiple EC2 instances behind an Application Load Balancer to host your application services and SNS which will act as a highly-scalable buffer that stores messages as they travel between distributed applications.

B. **Launch an Auto-Scaling group of EC2 instances to host your application services and an SQS queue. Include an Auto Scaling trigger to watch the SQS queue size which will either scale in or scale out the number of EC2 instances based on the queue.(Correct)**
C. Launch multiple EC2 instances behind an Application Load Balancer to host your application services, and SWF which will act as a highly-scalable buffer that stores messages as they travel between distributed applications.
D. Launch multiple On-Demand EC2 instances to host your application services and an SQS queue which will act as a highly-scalable buffer that stores messages as they travel between distributed applications.

EXPLANATION

There are three main parts in a distributed messaging system: the components of your distributed system which can be hosted on EC2 instance; your queue (distributed on Amazon SQS servers); and the messages in the queue.

To improve the scalability of your distributed system, you can add Auto Scaling group to your EC2 instances.

Question 44:

You deployed a web application to an EC2 instance that adds a variety of photo effects to a picture uploaded by the users. The application will put the generated photos to an S3 bucket by sending PUT requests to the S3 API.

What is the best option for this scenario considering that you need to have API credentials to be able to send a request to the S3 API?

A. Encrypt the API credentials and store in any directory of the EC2 instance.
B. **Create a role in IAM. Afterwards, assign this role to a new EC2 instance.(Correct)**
C. Store your API credentials in Amazon Glacier.
D. Store the API credentials in the root web application directory of the EC2 instance.

EXPLANATION

The best option is to create a role in IAM. Afterwards, assign this role to a new EC2 instance. Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances.

You can securely distribute your AWS credentials to the instances, enabling the applications on those instances to use your credentials to sign requests while protecting your credentials from other users. However, it's challenging to securely distribute credentials to each instance, especially those that AWS creates on your behalf such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your AWS credentials.

In this scenario, you have to use IAM roles so that your applications can securely make API requests from your instances without requiring you to manage the security credentials that the applications use. Instead of creating and distributing your AWS credentials, you can delegate permission to make API requests using IAM roles.

Options 1 and 4 are . Though you can store and use the API credentials in the EC2 instance, it will be difficult to manage just as mentioned above. You have to use IAM Roles.

Option 3 is as Amazon Glacier is used for data archives and not for managing API credentials.

Question 45:

You are working as an IT Consultant for a top investment firm. Your task is to ensure smooth upgrade of their accounting system in AWS to a new version without any system outages. The Technical Manager gave an advice to implement an in-place upgrade strategy while a DevOps Engineer suggested to use Blue/Green Deployment strategy instead.

Which of the following options are not the advantages of using Blue/Green Deployment over in-place upgrade strategy?

A. Blue/green deployments provide a level of isolation between your blue and green application environments, which reduce the deployment risk. The blue environment represents the current application version serving production traffic while the green one is staged running a different or upgrade version of your application.
B. It has the ability to simply roll the incoming traffic back to the currently working environment, in case of system failures, any time during the deployment process.
C. You can use Blue/Green Deployment with CodeCommit and CodeBuild to automatically deploy the new version of your application. (Correct)
D. Impaired operation or downtime is minimized because impact is limited to the window of time between green environment issue detection and shift of traffic back to the blue environment.
E. Blue/green deployment is more cost-effective than in-place upgrade. You don't need to launch a new environment with additional AWS resources. (Correct)

EXPLANATION

All of the options are advantages of Blue/Green deployments, except for Options 3 and 5. Take note that the Blue/Green deployment sets up a new green environment which uses entirely new AWS resources. In addition, CodeCommit and CodeBuild are not used for deployment and hence, it does not relate with Blue/Green deployments.

Traditionally, with in-place upgrades, it was difficult to validate your new application version in a production deployment while also continuing to run your old version of the application. Blue/green deployments provide a level of isolation between your blue and green application environments. It ensures that spinning up a parallel green environment does not affect resources underpinning your blue environment. This isolation reduces your deployment risk.

After you deploy the green environment, you have the opportunity to validate it. You might do that with test traffic before sending production traffic to the green environment, or by using a very small fraction of production traffic, to better reflect real user traffic. This is called canary analysis or canary testing. If you discover the green environment is not operating as expected, there is no impact on the blue environment. You can route traffic back to it, minimizing impaired operation or downtime, and limiting the blast radius of impact.

This ability to simply roll traffic back to the still-operating blue environment is a key benefit of blue/green deployments. You can roll back to the blue environment at any time during the deployment process. Blue/green deployments also fit well with continuous integration and continuous deployment (CI/CD) workflows, in many cases limiting their complexity. Your deployment automation would have to consider fewer dependencies on an existing environment, state, or configuration.

In AWS, blue/green deployments also provide cost optimization benefits. You're not tied to the same underlying resources. So if the performance envelope of the application changes from one version to another, you simply launch the new environment with optimized resources, whether that means fewer resources or just different compute resources. You also don't have to run an overprovisioned architecture for an extended period of time.

Question 46:

You have several EC2 Reserved Instances in your account that needs to be decommissioned and shut down since they are no longer required. The data is still required by the Audit team.

Which of the following steps can be taken for this scenario?

A. Convert the EC2 instance to On-Demand instances
B. You can opt to sell these EC2 instances on the AWS Reserved Instance Marketplace (Correct)
C. Take snapshots of the EBS volumes and terminate the EC2 instances. (Correct)

D. Convert the EC2 instances to Spot instances with a persistent Spot request type.

EXPLANATION

You can create a snapshot of the instance to save its data and then sell the instance to the Reserved Instance Marketplace.

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 length 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.

Question 47:

Your IT Manager asks you to create a decoupled application whose process includes dependencies on EC2 instances and servers located in your company's on-premises data center.

Which of these options are you least likely to recommend as part of that process?

A. SQS polling from an EC2 instance deployed with an IAM role
B. An SWF workflow
C. SQS polling from an EC2 instance using IAM user credentials(Correct)
D. Establish a Direct Connect connection from your on-premises network and VPC

EXPLANATION

For decoupled applications, it is best to use SWF and SQS which are both available in all options. Note that this question asks you for the option that you would LEASTlikely to recommend.

If you notice the 3rd option, it uses IAM user credentials for the EC2 instances which is not the recommended way to do so. It should use an IAM role instead. Hence, the correct answer is option 3.

Options 1, 2 and 4 are the recommended steps to satisfy the given requirement. You have to establish first a Direct Connect connection from your data center to your VPC to allow the on-premises servers to connect to SQS. You can either use SWF or SQS to create a decoupled application and you have to use an IAM Role, not an IAM user credential, on the EC2 instance to allow polling to the SQS queue.

Question 48:

You are working for a weather station in Asia with a weather monitoring system that needs to be migrated to AWS. Since the monitoring system requires a low network latency, high network throughput, you decided to launch your EC2 instances to a cluster placement group. However, when you try to add new instances to the new placement group, you receive an 'insufficient capacity error'.

How will you fix this issue?

A. **Stop and restart the instances in the Placement Group and then try the launch again.(Correct)**
B. Create another Placement Group and launch the new instances in the new group.
C. Verify all running instances are of the same size and type and then try the launch again.
D. Submit a capacity increase request to AWS as you are initially limited to only 12 instances per Placement Group.

EXPLANATION

It is recommended that you launch the number of instances that you need in the placement group in a single launch request and that you use the same instance type for all instances in the placement group. If you try to add more instances to the placement group later, or if you try to launch more than one instance type in the placement group, you increase your chances of getting an insufficient capacity error.

If you stop an instance in a placement group and then start it again, it still runs in the placement group. However, the start fails if there isn't enough capacity for the instance.

If you receive a capacity error when launching an instance in a placement group that already has running instances, stop and start all of the instances in the placement group, and try the launch again. Restarting the instances may migrate them to hardware that has capacity for all the requested instances.

Option 1 is correct because you can resolve this issue just by launching again. If the instances are stopped and restarted, AWS may move the instances to a hardware that has capacity for all the requested instances.

Option 2 is because to benefit from the enhanced networking, all the instances should be in the same Placement Group. Launching the new ones in a new Placement Group will not work in this case.

Option 3 is because the capacity error is not related to the instance size.

Option 4 is because there is no such limit on the number of instances in a Placement Group.

Question 49:

A large Philippine-based Business Process Outsourcing company is building a two-tier web application in their VPC to serve dynamic transaction-based content. The data tier is leveraging an Online Transactional Processing (OLTP) database but for the web tier, they are still deciding what service they will use.

What AWS services should you leverage to build an elastic and scalable web tier?

A. **Elastic Load Balancing, Amazon EC2, and Auto Scaling(Correct)**
B. Elastic Load Balancing, Amazon RDS with Multi-AZ, and Amazon S3
C. Amazon RDS with Multi-AZ and Auto Scaling
D. Amazon EC2, Amazon DynamoDB, and Amazon S3

EXPLANATION

Amazon RDS is a suitable database service for online transaction processing (OLTP) applications. However, the question asks for a list of AWS services for the web tier and not the database tier. Also, when it comes to services providing scalability and elasticity for your web tier, Auto Scaling and Elastic Load Balancer should immediately come into mind. Therefore, Option 1 is the correct answer.

To build an elastic and a highly-available web tier, you can use Amazon EC2, Auto Scaling, and Elastic Load Balancing. You can deploy your web servers on a fleet of EC2 instances to an Auto Scaling group, which will automatically monitor your applications and automatically adjust capacity to maintain steady, predictable performance at the lowest possible cost. Load balancing is an effective way to increase the availability of a system. Instances that fail can be replaced seamlessly behind the load balancer while other instances continue to operate. Elastic Load Balancing can be used to balance across instances in multiple availability zones of a region.

Options 2, 3 and 4 are since they don't mention all of the required services in building a highly available and scalable web tier, such as EC2, Auto Scaling, and Elastic Load Balancer. Although Amazon RDS with Multi-AZ and DynamoDB are highly scalable databases, the scenario is more focused on building its web tier and not the database tier.

Question 50:

You are a Solutions Architect in an intelligence agency that is currently hosting a learning and training portal in AWS. Your manager instructed you to launch a large EC2 instance with an attached EBS Volume and enable Enhanced Networking. What are the valid case scenarios in using Enhanced Networking?

A. **When you need a higher packet per second (PPS) performance(Correct)**

B. When you need a low packet-per-second performance
C. When you need high latency networking
D. When you need a consistently lower inter-instance latencies(Correct)
E. When you need a dedicated connection to your on-premises data center

EXPLANATION

Enhanced networking uses single root I/O virtualization (SR-IOV) to provide high-performance networking capabilities on supported instance types. SR-IOV is a method of device virtualization that provides higher I/O performance and lower CPU utilization when compared to traditional virtualized network interfaces. Enhanced networking provides higher bandwidth, higher packet per second (PPS) performance, and consistently lower inter-instance latencies. There is no additional charge for using enhanced networking.

Option 2 is because you want to increase packet-per-second performance, and not lower it, when you enable enhanced networking.

Option 3 is because higher latencies means slower network, which is the opposite of what you want to happen when you enable enhanced networking.

Option 5 is because enabling enhanced networking does not provide a dedicated connection to your on-premises data center. Use AWS Direct Connect or enable VPN tunneling instead for this purpose.

Question 51:

You have designed and built a new AWS architecture. After deploying your application to an On-demand EC2 instance, you found that there is an issue in your application when connecting to port 443. After troubleshooting the issue, you added port 443 to the security group of the instance.

How long will it take before the changes are applied to all of the resources in your VPC?

A. Roughly around 5-8 minutes in order for the security rules to propagate.
B. Immediately after a reboot of the EC2 instances which belong to that security group.
C. Immediately. (Correct)
D. It takes exactly one minute for the rules to apply to all availability zones within the AWS region.

EXPLANATION

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC could be assigned to a different set of security groups. If you don't specify a particular group at launch time, the instance is automatically assigned to the default security group for the VPC.

Option 3 is the correct answer. Changes made in a security group are immediately implemented. There is no need to wait for some amount of time for propagation nor reboot any instances for your changes to take effect.

Options 1 and 4 are because the changes in your security group are implemented immediately and not after a minute or after a few minutes.

Option 2 is because there is no need to reboot your EC2 instance before the security group changes are fully applied. The change takes effect immediately.

Question 52:

A startup is building an AI-based face recognition application in AWS, where they store millions of images in an S3 bucket. As the Solutions Architect, you have to ensure that each and every image uploaded to their system is stored without any issues.

What is the correct indication that an object was successfully stored when you put objects in Amazon S3?

A. **HTTP 200 result code and MD5 checksum. (Correct)**
B. Amazon S3 has 99.999999999% durability hence, there is no need to confirm that data was inserted.
C. You will receive an SMS from Amazon SNS informing you that the object is successfully stored.
D. You will receive an email from Amazon SNS informing you that the object is successfully stored.

EXPLANATION

If you triggered an S3 API call and got HTTP 200 result code and MD5 checksum, then it is considered as a successful upload. The S3 API will return an error code in case the upload is unsuccessful.

Option 2 is because although S3 is durable, it is not an assurance that all objects uploaded using S3 API calls will be successful.

Options 3 and 4 are because you don't receive an SMS nor an email notification by default, unless you added an event notification.

Question 53:

A WordPress website hosted in an EC2 instance, which has an additional EBS volume attached, was mistakenly deployed in the us-east-1a Availability Zone due to a misconfiguration in your CloudFormation template. There is a requirement to quickly rectify the issue by moving and attaching the EBS volume to a new EC2 instance in the us-east-1b Availability Zone.

As the Solutions Architect of the company, which of the following should you do to solve this issue?

A. Create a new EBS volume in another Availability Zone and then specify the current EBS volume as the source.
B. Detach the EBS volume and attach it to an EC2 instance residing in another Availability Zone.
C. First, create a snapshot of the EBS volume. Afterwards, create a volume using the snapshot in the other Availability Zone.(Correct)
D. First, create a new volume in the other Availability Zone. Next, perform a disk copy of the contents from the source volume to the new volume that you have created.

EXPLANATION

The first step is to create a snapshot of the EBS volume. Create a volume using this snapshot and then specify the new Availability Zone accordingly.

A point-in-time snapshot of an EBS volume, can be used as a baseline for new volumes or for data backup. If you make periodic snapshots of a volume, the snapshots are incremental—only the blocks on the device that have changed after your last snapshot are saved in the new snapshot. Even though snapshots are saved incrementally, the snapshot deletion process is designed so that you need to retain only the most recent snapshot in order to restore the entire volume.

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.

Option 1 is . There is no such action like this in AWS since EBS volumes do not require a source from other EBS volumes.

Option 2 is because an EBS volume is only available in the Availability Zone it was created in and cannot be attached directly to other Availability Zones.

Option 4 is because doing that is not the safest way to copy EBS contents. Create a snapshot instead for better reliability of the process.

Question 54:

There is a technical requirement by a financial firm that does online credit card processing to have a secure application environment on AWS. They are trying to decide on whether to use KMS or CloudHSM.

Which of the following statements is right when it comes to CloudHSM and KMS?

A. No major difference. They both do the same thing.
B. AWS CloudHSM does not support the processing, storage, and transmission of credit card data by a merchant or service provider, as it has not been validated as being compliant with Payment Card Industry (PCI) Data Security Standard (DSS); hence, you will need to use KMS.
C. You should consider using AWS CloudHSM over AWS KMS if you require your keys stored in dedicated, third-party validated hardware security modules under your exclusive control.(Correct)
D. AWS CloudHSM should always be used for any payment transactions.

EXPLANATION

AWS Key Management Service (KMS) is a multi-tenant, managed service that allows you to use and manage encryption keys. AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud. Both services offer a high level of security for your cryptographic keys. AWS CloudHSM provides a dedicated, FIPS 140-2 Level 3 HSM under your exclusive control, directly in your Amazon Virtual Private Cloud (VPC).

You should consider using AWS CloudHSM over AWS KMS if you require:

- Keys stored in dedicated, third-party validated hardware security modules under your exclusive control.

- FIPS 140-2 compliance.

- Integration with applications using PKCS#11, Java JCE, or Microsoft CNG interfaces.

- High-performance in-VPC cryptographic acceleration (bulk crypto).

Question 55:

You recently created a brand new IAM User with a default setting using AWS CLI. This is intended to be used to send API requests to your S3, DynamoDB, Lambda, and other AWS resources of your cloud infrastructure.

Which of the following must be done to allow the user to make API calls to your AWS resources?

A. Do nothing as the IAM User is already capable of sending API calls to your AWS resources.
B. Enable Multi-Factor Authentication for the user.

C. Assign an IAM Policy to the user to allow it to send API calls.

D. Create a set of Access Keys for the user and attach the necessary permissions.(Correct)

EXPLANATION

You can choose the credentials that are right for your IAM user. When you use the AWS Management Console to create a user, you must choose to at least include a console password or access keys. By default, a brand new IAM user created using the AWS CLI or AWS API has no credentials of any kind. You must create the type of credentials for an IAM user based on the needs of your user.

Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK). Users need their own access keys to make programmatic calls to AWS from the AWS Command Line Interface (AWS CLI), Tools for Windows PowerShell, the AWS SDKs, or direct HTTP calls using the APIs for individual AWS services.

To fill this need, you can create, modify, view, or rotate access keys (access key IDs and secret access keys) for IAM users. When you create an access key, IAM returns the access key ID and secret access key. You should save these in a secure location and give them to the user.

Option 1 is because by default, a brand new IAM user created using the AWS CLI or AWS API has no credentials of any kind. Take note that in the scenario, you created the new IAM user using the AWS CLI and not via the AWS Management Console, where you must choose to at least include a console password or access keys when creating a new IAM user.

Option 2 is because enabling Multi-Factor Authentication for the IAM user will still not provide the required Access Keys needed to send API calls to your AWS resources. You have to grant the IAM user with Access Keys to meet the requirement.

Option 3 is because adding a new IAM policy to the new user will not grant the needed Access Keys needed to make API calls to the AWS resources.

Question 56:

A tech company is running two production web servers hosted on Reserved EC2 instances with EBS-backed root volumes. These instances have a consistent CPU load of 90%. Traffic is being distributed to these instances by an Elastic Load Balancer. In addition, they also have Multi-AZ RDS MySQL databases for their production, test, and development environments.

What recommendation would you make to reduce cost in this AWS environment without affecting availability and performance of mission-critical systems? Choose the best answer.

A. Consider using On-demand instances instead of Reserved EC2 instances
B. Consider not using a Multi-AZ RDS deployment for the development and test database (Correct)
C. Consider using Spot instances instead of reserved EC2 instances
D. Consider removing the Elastic Load Balancer

EXPLANATION

One thing that you should notice here is that the company is using Multi-AZ databases in all of their environments, including their development and test environment. This is costly and unnecessary as these two environments are not critical. It is better to use Multi-AZ for production environments to reduce costs, which is why option 2 is the correct answer.

Option 1 is because selecting Reserved instances is cheaper than On-demand instances for long term usage due to the discounts offered when purchasing reserved instances.

Option 3 is because the web servers are running in a production environment. Never use Spot instances for production level web servers unless you are sure that they are not that critical in your system. This is because your spot instances can be terminated once the maximum price goes over the maximum amount that you specified.

Option 4 is because the Elastic Load Balancer is crucial in maintaining the elasticity and reliability of your system.

Question 57:

You are working as a Solutions Architect in a well-funded financial startup. The CTO instructed you to launch a cryptocurrency mining server on a Reserved EC2 instance in us-east-1 region's private subnet which is using IPv6. Due to the financial data that the server contains, the system should be secured to avoid any unauthorized access and to meet the regulatory compliance requirements.

In this scenario, which VPC feature allows the EC2 instance to communicate to the Internet but prevents inbound traffic?

A. NAT Gateway
B. NAT instances
C. Egress-only Internet gateway(Correct)
D. Internet Gateway

EXPLANATION

An egress-only Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows outbound communication over IPv6 from instances in your VPC to the Internet, and prevents the Internet from initiating an IPv6 connection with your instances.

Take note that an egress-only Internet gateway is for use with IPv6 traffic only. To enable outbound-only Internet communication over IPv4, use a NAT gateway instead.

Options 1 and 2 are because NAT gateways and NAT instances are only applicable for IPv4 and not IPv6. Even though these two components can enable the EC2 instance in a private subnet to communicate to the Internet and prevent inbound traffic, it is only limited with instances which are using IPv4 address and not IPv6. The most suitable VPC component to use is egress-only Internet gateway.

Option 4 is because Internet gateways are primarily used to provide Internet access to your instances in the public subnet of your VPC, and not for private subnets. However, with an Internet gateway, traffic originating from the public Internet will also be able to reach your instances. The scenario is asking you to prevent inbound access, so this is not the correct answer.

Question 58:

An AWS account has an ID of 0499802888. Which of the following URLs would you provide to the IAM user to be able to access the AWS Console?

A. **https://0499802888.signin.aws.amazon.com/console(Correct)**
B. https://signin.0499802888.aws.amazon.com/console
C. https://signin.aws.amazon.com/console
D. https://aws.amazon.com/console

EXPLANATION

To use the AWS Management Console, IAM users must provide their account ID or account alias in addition to their username and password. When you, as an administrator, create an IAM user in the console, you must send the sign-in credentials to that user, including the username and the URL to the account sign-in page.

Your unique account sign-in page URL is created automatically when you begin using IAM. You do not have to do anything to use this sign-in page. You can also customize the account sign-in URL for your account if you want the URL to contain your company name (or other friendly identifier) instead of your AWS account ID number.

AWS sign-in page URL format:

https://My_AWS_Account_ID.signin.aws.amazon.com/console/

Option 2 is because your account ID should come first before the word signin. Here is a technique to help you remember this format: you should always come first since you own this account.

Option 3 is because this only redirects you to the sign in page where you will have to enter your account ID or alias manually. If the person you invited to the account is not aware of the account ID then he/she will not be able to log into the account.

Option 4 is because this link redirects you to the details of what a console is.

Question 59:

You have a fleet of running Spot EC2 instances behind an Application Load Balancer. The incoming traffic comes from various users across multiple AWS regions and you would like to have the user's session shared among your fleet of instances. You are required to set up a distributed session management layer that will provide a scalable and shared data storage for the user sessions.

Which of the following would be the best choice to meet the requirement while still providing sub-millisecond latency for your users?

A. ELB sticky sessions
B. Multi-master DynamoDB
C. Multi-AZ RDS
D. ElastiCache in-memory caching(Correct)

EXPLANATION

For sub-millisecond latency caching, ElastiCache is the best choice. In order to address scalability and to provide a shared data storage for sessions that can be accessed from any individual web server, you can abstract the HTTP sessions from the web servers themselves. A common solution to for this is to leverage an In-Memory Key/Value store such as Redis and Memcached.

Option 1 is because the scenario does not require you to route a user to the particular web server that is managing that individual user's session. Since the session state is shared among the instances, the use of the ELB sticky sessions feature is not recommended in this scenario.

Options 2 and 3 are because although you can use DynamoDB and RDS for storing session state, these two are not the best choices in terms of cost-effectiveness and performance when compared to ElastiCache. There is a significant difference in terms of latency if you used DynamoDB and RDS when you store the session data.

Question 60:

You are working for a startup that builds Internet of Things (IOT) devices and monitoring application. They are using IOT sensors to monitor all data by using Amazon Kinesis configured with default settings. You then send the data to an Amazon S3 bucket after 2 days. When you checked the data in S3, there are only data for the last day and nothing for the first day.

What is the root cause of this issue?

A. Amazon S3 bucket has encountered a data loss.
B. Someone has manually deleted the record in Amazon S3.
C. By default, data records in Kinesis are only accessible for 24 hours from the time they are added to a stream.(Correct)
D. The access of the Kinesis stream to the S3 bucket is insufficient.

EXPLANATION

By default, records of a stream in Amazon Kinesis are accessible for up to 24 hours from the time they are added to the stream. You can raise this limit to up to 7 days by enabling extended data retention. Hence, Option 3 is correct.

Option 1 is because Amazon S3 rarely experiences data loss. Amazon has an SLA for S3 that it commits to its customers. Amazon S3 Standard, S3 Standard–IA, S3 One Zone-IA, and S3 Glacier are all designed to provide 99.999999999% durability of objects over a given year. This durability level corresponds to an average annual expected loss of 0.000000001% of objects. Hence, Amazon S3 bucket data loss is highly unlikely.

Option 2 is because if someone has deleted the data, this should have been visible in CloudTrail. Also, deleting that much data manually shouldn't have occurred in the first place if you have put in the appropriate security measures.

Option 4 is because having insufficient access is highly unlikely since you are able to access the bucket and view the contents of the previous day's data collected by Kinesis.

Question 61:

You are working as the Solutions Architect for a global technology consultancy firm which has an application that uses multiple EC2 instances located in various AWS regions such as US East (Ohio), US West (N. California), and EU (Ireland). Your manager instructed you to set up a latency-based routing to route incoming traffic for www.tutorialsdojo.com to all the EC2 instances across all AWS regions.

Which of the following options can satisfy the given requirement?

A. Use a Network Load Balancer to distribute the load to the multiple EC2 instances across all AWS Regions.
B. Use Route 53 to distribute the load to the multiple EC2 instances across all AWS Regions.(Correct)
C. Use an Application Load Balancer to distribute the load to the multiple EC2 instances across all AWS Regions.
D. This is not possible in AWS. You can only set up a latency-based routing in one AWS region.

EXPLANATION

If your application is hosted in multiple AWS Regions, you can improve performance for your users by serving their requests from the AWS Region that provides the lowest latency.

You can create latency records for your resources in multiple AWS Regions by using latency-based routing. In the event that Route 53 receives a DNS query for your domain or subdomain such as tutorialsdojo.com or portal.tutorialsdojo.com, it determines which AWS Regions you've created latency records for, determines which region gives the user the lowest latency and then selects a latency record for that region. Route 53 responds with the value from the selected record which can be the IP address for a web server or the CNAME of your elastic load balancer. Hence, Option 2 is correct.

Options 1 and 3 are because load balancers distribute traffic only within their respective regions and not to other AWS regions. It is best to use Route 53 instead to balance the incoming load to two or more AWS regions.

Option 4 is as the requirement can be addressed with Route 53 latency-based routing.

Question 62:

You are working for a startup which develops an AI-based traffic monitoring service. You need to register a new domain called www.tutorialsdojo-ai.com and set up other DNS entries for the other components of your system in AWS. Which of the following is not supported by Amazon Route 53?

A. DNSSEC (Domain Name System Security Extensions)(Correct)
B. PTR (pointer record)
C. SPF (sender policy framework)
D. SRV (service locator)

EXPLANATION

Amazon Route 53’s DNS services does not support DNSSEC at this time. However, their domain name registration service supports configuration of signed DNSSEC keys for domains when DNS service is configured at another provider. More information on configuring DNSSEC for your domain name registration can be found here.

Amazon Route 53 currently supports the following DNS record types:

- -A (address record)
- -AAAA (IPv6 address record)
- -CNAME (canonical name record)
- -CAA (certification authority authorization)
- -MX (mail exchange record)
- -NAPTR (name authority pointer record)
- -NS (name server record)
- -PTR (pointer record)
- -SOA (start of authority record)
- -SPF (sender policy framework)
- -SRV (service locator)
- -TXT (text record)

Question 63:

A new DevOps engineer has created a CloudFormation template for a web application and she raised a pull-request in GIT for you to check and review. After checking the template, you immediately told her that the template will not work.

Which of the following is the reason why this CloudFormation template will fail to deploy the stack?

```
{ "AWSTemplateFormatVersion":"2010-09-09",
  "Parameters":{
    "VPCId":{
      "Type":"String",
      "Description":"tutorialsdojo"
    },
    "SubnetId":{
      "Type":"String",
      "Description":"subnet-b46032ec"
    }
  },
  "Outputs":{
    "InstanceId":{
      "Value":{
        "Ref":"TutorialsDojoInstance"
      }, "Description":"Instance Id"
    }
   }
 }
```

A. The value of the AWSTemplateFormatVersion is . It should be 2017-06-06.
B. The Resources section is missing.(Correct)
C. An invalid section named Parameters is present. This will cause the CloudFormation stack to fail.
D. The Conditions section is missing.

EXPLANATION

In CloudFormation, a template is a JSON or a YAML-formatted text file that describes your AWS infrastructure. Templates include several major sections. The Resources section is the only required section. Some sections in a template can be in any order. However, as you build your template, it might be helpful to use the logical ordering of the following list, as values in one section might refer to values from a previous section. Take note that all of the sections here are optional, except for Resources, which is the only one required.

- -Format Version
- -Description
- -Metadata
- -Parameters
- -Mappings
- -Conditions
- -Transform
- -Resources (required)

- -Outputs

Question 64:

A construction company has an online system that tracks all of the status and progress of their projects. The system is hosted in AWS and there is a requirement to monitor the read and write IOPs metrics for their MySQL RDS instance and send real-time alerts to their DevOps team.

Which of the following services in AWS can you use to meet the requirements?

A. SWF
B. CloudWatch(Correct)
C. Amazon Simple Queue Service
D. Route 53
E. Amazon Simple Notification Service(Correct)

EXPLANATION

In this scenario, you can use CloudWatch to monitor your AWS resources and SNS to provide notification. Hence, the correct answers are Options 2 and 5.

Amazon Simple Notification Service (SNS) is a flexible, fully managed pub/sub messaging and mobile notifications service for coordinating the delivery of messages to subscribing endpoints and clients.

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources.

Option 1 is because SWF is mainly used for managing workflows and not for monitoring and notifications.

Option 3 is because SQS is a messaging queue service and not suitable for this kind of scenario.

Option 4 is because Route 53 is primarily used for routing and domain name registration and management.

Question 65:

You are implementing a hybrid network architecture where you will be using Amazon S3 as your primary data storage, while retaining frequently accessed data locally in your storage gateway. The objective is to minimize the need to scale your on-premises storage infrastructure while still providing your applications with low-latency access to their frequently accessed data.

Which type of AWS Storage Gateway is the best to use for this scenario?

A. File Gateway
B. Cached Volume Gateway(Correct)
C. Stored Volume Gateway
D. Virtual tape library (VTL)

EXPLANATION

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 their frequently accessed data. You can create storage volumes up to 32 TiB in size and attach to them as iSCSI devices from your on-premises application servers. Your gateway stores data that you write to these volumes in Amazon S3 and retains recently read data in your on-premises storage gateway's cache and upload buffer storage.