AWS Practice Questions (Paper 2)

Question 1:

You are a Solutions Architect working with a company that uses Chef Configuration management in their datacenter. Which service is designed to let the customer leverage existing Chef recipes in AWS?

- **A.** Amazon Simple Workflow Service
- B. Aws Elastic Beanstalk
- C. AWS Cloud Formation
- **D. AWS OpsWorks(Correct)**

EXPLANATION

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

Option 1 is because AWS SWF is a fully-managed state tracker and task coordinator in the Cloud. It does not let you leverage Chef recipes.

Option 2 is because Elastic Beanstalk handles an application's deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring. It does not let you leverage Chef recipes just like Option 1.

Option 3 is because CloudFormation is a service that lets you create a collection of related AWS resources and provision them in a predictable fashion using infrastructure as code. It does not let you leverage Chef recipes just like Options 1 and 2.

Question 2:

You work for a leading university as an AWS Infrastructure Engineer and also as a professor to aspiring AWS architects. As a way to familiarize your students with AWS, you gave them a project to host their applications to an EC2 instance. One of your students created an instance to host their online enrollment system project but is having a hard time connecting to their newly created EC2 instance. Your students have explored all of the troubleshooting guides by AWS and narrowed it down to login issues.

- A. Custom EC2 password
- B. EC2 Connection Strings
- **C. Key Pairs(Correct)**

D. Access Keys

EXPLANATION

Amazon EC2 uses public–key cryptography to encrypt and decrypt login information. Public–key cryptography uses a public key to encrypt a piece of data, such as a password, then the recipient uses the private key to decrypt the data. The public and private keys are known as a key pair.

To log in to your instance, you must create a key pair, specify the name of the key pair when you launch the instance, and provide the private key when you connect to the instance. On a Linux instance, the public key content is placed in an entry within ~/.ssh/authorized_keys. This is done at boot time and enables you to securely access your instance using the private key instead of a password.

Options 1 and 2 are as both Custom EC2 password and EC2 Connection Strings do not exist.

Option 4 is as Access Keys are used for API calls and not for logging in to EC2.

Question 3:

You are working as an IT consultant for a major telecommunications company. They have an application using an Oracle database deployed in a large EC2 instance which is used for their infrequently accessed data. In this scenario, what is the most cost-effective storage type for the EC2 instance that hosts the database?

A. EBS general purpose SSD
B. Provisioned IOPS SSD
C. Throughput optimized HDD
D. Cold HDD(Correct)

EXPLANATION

Cold HDD volumes provide low-cost magnetic storage that defines performance in terms of throughput rather than IOPS. With a lower throughput limit than Throughput Optimized HDD, this is a good fit ideal for large, sequential cold-data workloads. If you require infrequent access to your data and are looking to save costs, Cold HDD provides inexpensive block storage. Take note that bootable Cold HDD volumes are not supported.

Cold HDD provides the lowest cost HDD volume and is designed for less frequently accessed workloads. Hence, Option 4 is the correct answer.

In the exam, always consider the difference between SSD and HDD as shown on the table below. This will allow you to easily eliminate specific EBS-types in the options which are not SSD or not HDD, depending on whether the question asks for a

storage type which has small, random I/O operations or large, sequential I/O operations.

Option 1 is because a General purpose SSD volume costs more and it is mainly used for a wide variety of workloads. It is recommended to be used as system boot volumes, virtual desktops, low-latency interactive apps, and many more.

Option 2 is because Provisioned IOPS HDD costs more than the Cold HDD and thus, not cost-effective for this scenario. It provides the highest performance SSD volume for mission-critical low-latency or high-throughput workloads, which is not needed in the scenario.

Option 3 is because Throughput Optimized HDD is primarily used for frequently accessed, throughput-intensive workloads. In this scenario, Cold HDD perfectly fits the requirement as it is used for their infrequently accessed data and provides the lowest cost, unlike Throughput Optimized HDD.

Question 4:

You are building a transcription service for a company in which a fleet of EC2 worker instances process an uploaded audio file and generate a text file as an output. You must store both of these files in the same durable storage until the text file is retrieved by the uploader. Due to an expected surge in demand, you have to ensure that the storage is scalable.

Which storage option in AWS can you use in this situation, which is both cost-efficient and scalable?

A. Multiple Amazon EBS volume with snapshots
B. A single Amazon Glacier vault
C. A single Amazon S3 bucket (Correct)
D. Multiple instance stores

EXPLANATION

In this scenario, the best option is to use Amazon S3. It’s a simple storage service that offers a highly-scalable, reliable, and low-latency data storage infrastructure at very low costs.

Options 1 and 4 are because these services do not provide durable storage.

Option 2 is because Amazon Glacier is mainly used for data archives with data retrieval times that can take some few hours. Hence, it is not suitable for the transcription service where the data are stored and frequently accessed.

Question 5:

As an AWS Cloud Consultant working for a record company, you are building an application that will store both key-value store and document models like band ID, album ID, song ID and composer ID.

Which AWS service will suit your needs for your application?

- **A.** AWS RDS
- **B. Dynamo DB(Correct)**
- C. Oracle RDS
- D. Elastic Map Reduce

EXPLANATION:

Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. It is a fully managed cloud database and supports both document and key-value store models. Its flexible data model, reliable performance, and automatic scaling of throughput capacity makes it a great fit for mobile, web, gaming, ad tech, IoT, and many other applications.

Option 1 is because RDS is a relational database while DynamoDB is non-relational.

Option 3 is because Oracle RDS itself is a relational database.

Option 4 is because it is used for large scale data warehouse service for use with business intelligence tools.

Question 6:

The operations team of your company asked you for a way to monitor the health of your production EC2 instances in AWS. You told them to use the CloudWatch service.

Which of the following metrics is not available by default in CloudWatch?

- A. CPU Usage
- **B. Memory Usage(Correct)**
- C. Disk Read operations
- D. Network In and Out

EXPLANATION

Memory Usage is a metric not available by default in CloudWatch. You need to add a custom metric for it to work.

Question 7:

A startup company has a serverless architecture that uses AWS Lambda, API Gateway, and DynamoDB. They received an urgent feature request from their client last month and now, it is ready to be pushed to production. The company is using AWS CodeDeploy as their deployment service.

Which of the following configuration types will allow you to specify the percentage of traffic shifted to your updated Lambda function version before the remaining traffic is shifted in the second increment?

A. Canary (Correct)
B. Linear
C. All-at-once
D. Blue/Green deployment

EXPLANATION

If you're using the AWS Lambda compute platform, you must choose one of the following deployment configuration types to specify how traffic is shifted from the original AWS Lambda function version to the new AWS Lambda function version:

Canary: Traffic is shifted in two increments. You can choose from predefined canary options that specify the percentage of traffic shifted to your updated Lambda function version in the first increment and the interval, in minutes, before the remaining traffic is shifted in the second increment.

Linear: Traffic is shifted in equal increments with an equal number of minutes between each increment. You can choose from predefined linear options that specify the percentage of traffic shifted in each increment and the number of minutes between each increment.

All-at-once: All traffic is shifted from the original Lambda function to the updated Lambda function version at once.

Question 8:

A media company has two VPCs: VPC-1 and VPC-2 with peering connection between each other. VPC-1 only contains private subnets while VPC-2 only contains public subnets. The company uses a single AWS Direct Connect connection and a virtual interface to connect their on-premises network with VPC-1.

Which of the following options increase the fault tolerance of the connection to VPC-1

A. Use the AWS VPN CloudHub to create a new AWS Direct Connect connection and private virtual interface in the same region as VPC-2.

B. Establish a hardware VPN over the Internet between VPC-1 and the on-premises network. (Correct)
C. Establish a hardware VPN over the Internet between VPC-2 and the on-premises network.
D. Establish a new AWS Direct Connect connection and private virtual interface in the same region as VPC-2.
E. Establish another AWS Direct Connect connection and private virtual interface in the same AWS region as VPC-1. (Correct)

EXPLANATION

In this scenario, you have two VPCs which have peering connections with each other. Note that a VPC peering connection does not support edge to edge routing. This means that if either VPC in a peering relationship has one of the following connections, you cannot extend the peering relationship to that connection:

- A VPN connection or an AWS Direct Connect connection to a corporate network

- An Internet connection through an Internet gateway

- An Internet connection in a private subnet through a NAT device

- A VPC endpoint to an AWS service; for example, an endpoint to Amazon S3.

- (IPv6) A ClassicLink connection. You can enable IPv4 communication between a linked EC2-Classic instance and instances in a VPC on the other side of a VPC peering connection. However, IPv6 is not supported in EC2-Classic, so you cannot extend this connection for IPv6 communication.

For example, if VPC A and VPC B are peered, and VPC A has any of these connections, then instances in VPC B cannot use the connection to access resources on the other side of the connection. Similarly, resources on the other side of a connection cannot use the connection to access VPC B.

Hence, this means that you cannot use VPC-2 to extend the peering relationship that exists between VPC-1 and the on-premises network. For example, traffic from the corporate network can't directly access VPC-1 by using the VPN connection or the AWS Direct Connect connection to VPC-2, which is why Options 1, 3, and 4 are .

The correct answers are options 2 and 5. You can do the following to provide a highly available, fault-tolerant network connection:

- Establish a hardware VPN over the Internet between the VPC and the on-premises network.

- Establish another AWS Direct Connect connection and private virtual interface in the same AWS region.

Question 9:

An online events registration system is hosted in AWS and uses ECS to host its front-end tier and a Multi-AZ RDS for its database tier, which also has a standby replica. What are the events that will make Amazon RDS automatically perform a failover to the standby replica?

A. **Loss of availability in primary Availability Zone(Correct)**
B. **Storage failure on primary(Correct)**
C. Storage failure on secondary DB instance
D. In the event of Read Replica failure
E. Compute unit failure on secondary DB instance

EXPLANATION

Amazon RDS detects and automatically recovers from the most common failure scenarios for Multi-AZ deployments so that you can resume database operations as quickly as possible without administrative intervention.

Amazon RDS automatically performs a failover in the event of any of the following:

Loss of availability in primary Availability Zone

Loss of network connectivity to primary

Compute unit failure on primary

Storage failure on primary

Options 3, 4 and 5 are because all these scenarios do not affect the primary database. Automatic failover only occurs if the primary database is the one that is affected.

Question 10:

One of your EC2 instances is reporting an unhealthy system status check. The operations team is looking for an easier way to monitor and repair these instances instead of fixing them manually. How will you automate the monitoring and repair of the system status check failure in an AWS environment?

A. **Create CloudWatch alarms that stop and start the instance based on status check alarms.(Correct)**
B. Write a python script that queries the EC2 API for each instance status check
C. Write a shell script that periodically shuts down and starts instances based on certain stats.

D. Buy and implement a third party monitoring tool.

EXPLANATION

Using Amazon CloudWatch alarm actions, you can create alarms that automatically stop, terminate, reboot, or recover your EC2 instances. You can use the stop or terminate actions to help you save money when you no longer need an instance to be running. You can use the reboot and recover actions to automatically reboot those instances or recover them onto new hardware if a system impairment occurs.

Options 2, 3 and 4 are because it is unnecessary to go through such lengths when CloudWatch Alarms already has such a feature for you, offered at a low cost.

Question 11:

As a Network Architect developing a food ordering application, you need to retrieve the instance ID, public keys, and public IP address of the EC2 server you made for tagging and grouping the attributes into your internal application running on-premises.

Which EC2 feature will help you achieve your requirements?

A. Instance user data
B. Resource tags
C. Instance metadata(Correct)
D. Amazon Machine Image

EXPLANATION

Instance metadata is the data about your instance that you can use to configure or manage the running instance. You can get the instance ID, public keys, public IP address and many other information from the instance metadata by firing a URL command in your instance to this URL:

http://169.254.169.254/latest/meta-data/

Option 1 is because the instance user data is mainly used to perform common automated configuration tasks and run scripts after the instance starts.

Option 2 is because resource tags are labels that you assign to an AWS resource. Each tag consists of a key and an optional value, both of which you define.

Option 4 is because Amazon Machine Image (AMI) mainly provides the information required to launch an instance, which is a virtual server in the cloud.

Question 12:

You are working for a central bank as the Principal AWS Solutions Architect. Due to compliance requirements and security concerns, you are tasked to implement strict access to the central bank's AWS resources using the AWS Identity and Access Management service.

Which of the following can you manage in the IAM dashboard?

A. **Groups(Correct)**
B. **Identity providers(Correct)**
C. Cost Allocation Reports
D. Security Groups
E. Network Access Control List

EXPLANATION

AWS Identity and Access Management (IAM) is a web service for securely controlling access to AWS services. With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users and applications can access.

Option 1 is correct because an IAM group is a collection of IAM users. Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users.

Option 2 is correct as you can manage identity providers using IAM Dashboard instead of creating IAM users in your AWS account. With an identity provider (IdP), you can manage your user identities outside of AWS and give these external user identities permission to use AWS resources in your account.

Option 3 is because cost allocation reports are under AWS Billing and Cost Management.

Option 4 is because security groups can be managed in the EC2 console and not in the IAM dashboard.

Option 5 is because Network ACL is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets while security groups act as virtual firewall for your instance to control inbound and outbound traffic, both of which cannot be managed in the IAM dashboard.

Question 13:

Your fellow AWS Engineer has created a new Standard-class S3 bucket to store financial reports that are not frequently accessed but should be immediately available when an auditor requests for it. To save costs, you

changed the storage class of the S3 bucket from Standard to Infrequent Access storage class.

In Amazon S3 Standard - Infrequent Access storage class, which of the following statements are true?

- **A. It is designed for data that is accessed less frequently.(Correct)**
- B. It is the best storage option to store noncritical and reproducible data
- **C. It is designed for data that requires rapid access when needed.(Correct)**
- D. It provides high latency and low throughput performance
- E. Ideal to use for data archiving.

EXPLANATION

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

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

Key Features:

- Same low latency and high throughput performance of Standard

- Designed for durability of 99.999999999% of objects

- Designed for 99.9% availability over a given year

- Backed with the Amazon S3 Service Level Agreement for availability

- Supports SSL encryption of data in transit and at rest

- Lifecycle management for automatic migration of objects

Option 2 is as it actually refers to Amazon S3 - Reduced Redundancy Storage (RRS). In addition, RRS will be completely deprecated soon and AWS recommends to use S3 IA One-Zone instead.

Option 4 is as it should be "low latency" and "high throughput" instead. S3 automatically scales performance to meet user demands.

Option 5 is because this statement refers to Amazon Glacier. Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup.

Question 14:

You are instructed by your manager to set up a bastion host to your Amazon VPC and that you should be the only person that can access it via SSH. What is the best way for you to achieve this?

A. Create a large EC2 instance with a security group which only allows access on port 22 using your own pre-configured password.
B. Create a large EC2 instance with a security group which only allows access on port 22 via your IP address.
C. Create a small EC2 instance with a security group which only allows access on port 22 using your own pre-configured password.
D. Create a small EC2 instance and a security group which only allows access on port 22 via your IP address.(Correct)

EXPLANATION

The best way to implement a bastion host is to create a small EC2 instance which should only have a security group from a particular IP address for maximum security. We use a small instance rather than a large one because this host will only act as a jump server to connect to other instances in your VPC and nothing else. Hence, there is no point of allocating a large instance simply because it doesn't need that much computing power to process SSH (port 22) or RDP (port 3389) connections. Hence, option 4 is the right answer for this scenario.

Options 1 and 3 are because even though you have your own pre-configured password, the SSH connection can still be accessed by anyone over the Internet, which poses as a security vulnerability.

Option 2 is because you don't need a large instance for a bastion host as it does not require much CPU resources.

Question 15:

You are building a cloud infrastructure where you have EC2 instances that require access to various AWS services such as S3 and Redshift. You will also need to provision access to system administrators so they can deploy and test their changes.

Which configuration should be used to ensure that AWS Credentials like Access Keys and Secret Access Keys are secured and not compromised?

A. Enable Multi-Factor Authentication.(Correct)
B. Assign an IAM role to the Amazon EC2 instance.(Correct)
C. Store the AWS Access Keys in the EC2 instance.
D. Assign an IAM user for each Amazon EC2 Instance.

E. Store the AWS Access Keys in ACM.

EXPLANATION

In this scenario, the correct answers are:

- Enable Multi-Factor Authentication

- Assign an IAM role to the Amazon EC2 instance

Always remember that you should associate IAM roles to EC2 instances and not an IAM user, for the purpose of accessing other AWS services. IAM roles are designed 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.

AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your user name and password. With MFA enabled, when a user signs in to an AWS website, they will be prompted for their user name and password (the first factor—what they know), as well as for an authentication code from their AWS MFA device (the second factor—what they have). Taken together, these multiple factors provide increased security for your AWS account settings and resources. You can enable MFA for your AWS account and for individual IAM users you have created under your account. MFA can also be used to control access to AWS service APIs.

Option 3 is because storing AWS access keys in an EC2 instance is not recommended by AWS, as it can be compromised. Instead of storing access keys on an EC2 instance for use by applications that run on the instance and make AWS API requests, you can use an IAM role to provide temporary access keys for these applications.

Option 4 is because there is no need to create an IAM user for this scenario since IAM roles already provide greater flexibility and easier management.

Option 5 is because ACM is just a service that lets you easily provision, manage, and deploy public and private SSL/TLS certificates for use with AWS services and your internal connected resources. It is not used as a secure storage for your access keys.

Question 16:

You want to establish an SSH connection to a Linux instance hosted in your VPC via the Internet. Which of the following is not required in order for this to work?

A. Secondary Private IP Address(Correct)
B. Public IP Address or Elastic IP

C. Internet Gateway
D. Network access control and security group rules which allow the relevant traffic to flow to and from your EC2 instance.

EXPLANATION

To SSH into your EC2 instance via the Internet, you need to ensure that your VPC has an attached Internet Gateway, so that your instance can reach the Internet. Your instance should also have either a public IP or Elastic IP address, depending on whether you need a persistent IP address or not. Also ensure that you have configured your security groups to allow SSH inbound.

You don't need a Secondary Private IP Address since this address is only used when communicating within your VPC and thus, one Private IP address is enough. Hence, Option 1 is correct.

To enable access to or from the Internet for instances in a VPC subnet, you must do the following:

- Attach an internet gateway to your VPC.

- Ensure that your subnet's route table points to the Internet gateway.

- Ensure that instances in your subnet have a globally unique IP address (public IPv4 address, Elastic IP address, or IPv6 address).

- Ensure that your network access control lists and security groups allow the relevant traffic to flow to and from your instance.

Question 17:

You are working as a Cloud Consultant for a government agency with a mandate of improving traffic planning, maintenance of roadways and preventing accidents. There is a need to manage traffic infrastructure in real time, alert traffic engineers and emergency response teams when problems are detected, and automatically change traffic signals to get emergency personnel to accident scenes faster by using sensors and smart devices.

Which AWS service will allow the developers of the agency to connect the said devices to your cloud-based applications?

A. CloudFormation
B. Elastic Beanstalk
C. AWS IoT Core(Correct)
D. Container service

EXPLANATION

AWS IoT Core is a managed cloud service that lets connected devices easily and securely interact with cloud applications and other devices. AWS IoT Core provides secure communication and data processing across different kinds of connected devices and locations so you can easily build IoT applications.

Option 1 is because CloudFormation is mainly used for creating and managing the architecture and not for handling connected devices. You have to use AWS IoT Core instead.

Option 2 is because AWS Elastic Beanstalk is mainly used as a substitute to Infrastructure-as-a-Service with Platform-as-a-Service, which reduces management complexity without restricting choice or control and not for handling connected devices.

Option 4 is because Amazon Elastic Container Services is mainly used for creating and managing docker instances and not for handling devices.

Question 18:

You need to back up your mySQL database hosted on a Reserved EC2 instance. It is using EBS volumes that are configured in a RAID array.

What steps will you take to minimize the time during which the database cannot be written to and to ensure a consistent backup?

1. Detach EBS volumes from the EC2 instance.

2. Start EBS snapshot of volumes.

3. Re-attach the EBS volumes.

1. Stop all applications from writing to the RAID array.

2. Flush all caches to the disk.

3. Confirm that the associated EC2 instance is no longer writing to the RAID array by taking actions such as freezing the file system, unmounting the RAID array, or even shutting down the EC2 instance.

4. **After taking steps to halt all disk-related activity to the RAID array, take a snapshot of each EBS volume in the array.(Correct)**

1. Stop all I/O activity in the volumes.

2. Create an image of the EC2 Instance.

3. Resume all I/O activity in the volume.

1. Stop all I/O activity in the volumes.

2. Start EBS snapshot of volumes.

3. While the snapshot is in progress, resume all I/O activity.

EXPLANATION

Remember that since the instance is using a RAID configuration, the snapshot process is different. You should stop all I/O activity of the volumes before creating a snapshot. Hence, option 2 is correct:

Stop all applications from writing to the RAID array.

Flush all caches to the disk.

Confirm that the associated EC2 instance is no longer writing to the RAID array by taking actions such as freezing the file system, unmounting the RAID array, or even shutting down the EC2 instance.

After taking steps to halt all disk-related activity to the RAID array, take a snapshot of each EBS volume in the array.

When you take a snapshot of an attached Amazon EBS volume that is in use, the snapshot excludes data cached by applications or the operating system. For a single EBS volume, this is often not a problem. However, when cached data is excluded from snapshots of multiple EBS volumes in a RAID array, restoring the volumes from the snapshots can degrade the integrity of the array.

When creating snapshots of EBS volumes that are configured in a RAID array, it is critical that there is no data I/O to or from the volumes when the snapshots are created. RAID arrays introduce data interdependencies and a level of complexity not present in a single EBS volume configuration.

Option 1 is as you don't need to detach the volumes in the first place.

Option 3 is as you don't need to create a new image of the instance.

Option 4 is because there are missing steps in the process. You have to flush all caches to the disk first and you have to ensure that the EC2 instance is no longer writing to the RAID Array.

Question 19:

You are developing a meal planning application that provides meal recommendations for the week as well as the food consumption of your users.

Your application resides on an EC2 instance which requires access to various AWS services for its day-to-day operations.

Which of the following is the best way to allow your EC2 instance to access your S3 bucket and other AWS services?

1. **Create a role in IAM and assign it to the EC2 instance.(Correct)**
2. Store the API credentials in the EC2 instance.
3. Add the API Credentials in the Security Group and assign it to the EC2 instance.
4. Store the API credentials in a bastion host.

EXPLANATION

The best practice in handling API Credentials is to create a new role in the Identity Access Management (IAM) service and then assign it to a specific EC2 instance. In this way, you have a secure and centralized way of storing and managing your credentials.

Options 2, 3, and 4 are because it is not secure to store nor use the API credentials from an EC2 instance. You should use IAM service instead.

Question 20:

Your company just recently adopted a hybrid architecture that integrates their on-premises data center to their AWS cloud. You are assigned to configure the VPC as well as to implement the required IAM users, IAM roles, IAM groups and IAM policies.

In this scenario, what is a best practice when creating IAM policies?

A. **Use the principle of least privilege which means granting only the permissions required to perform a task.(Correct)**
B. Grant all permissions to any EC2 user.
C. Use the principle of least privilege which means granting only the least number of people with full root access.
D. Determine what users need to do and then craft policies for them that let the users perform those tasks including additional administrative operations.

EXPLANATION

One of the best practices in Amazon IAM is to grant least privilege.

When you create IAM policies, follow the standard security advice of granting least privilege—that is, granting only the permissions required to perform a task.

Determine what users need to do and then craft policies for them that let the users perform only those tasks. Therefore, option 1 is the correct answer.

Start with a minimum set of permissions and grant additional permissions as necessary.

Defining the right set of permissions requires some understanding of the user's objectives. Determine what is required for the specific task, what actions a particular service supports, and what permissions are required in order to perform those actions.

Option 2 is , since you don't want your users to gain access to everything and perform unnecessary actions. Doing so is not a good security practice.

Option 3 is because granting only the least number of people with full root access is not the correct definition of what the principle of least privilege is.

Option 4 is as well since there are some users who you should not give administrative access to. You should follow the principle of least privilege when providing permissions and accesses to your resources.

Question 21:

You are working as a Solutions Architect for a start-up company that has a not-for-profit crowdfunding platform hosted in AWS. Their platform allows people around the globe to raise money for social enterprise projects including challenging circumstances like accidents and illnesses. Since the system handles financial transactions, you have to ensure that your cloud architecture is secure.

Which of the following AWS services encrypts data at rest by default?

A. **AWS Storage Gateway(Correct)**
B. Amazon RDS
C. Amazon ECS
D. **Amazon Glacier(Correct**)
E. AWS Lambda

EXPLANATION

All data transferred between any type of gateway appliance and AWS storage is encrypted using SSL. By default, all data stored by AWS Storage Gateway in S3 is encrypted server-side with Amazon S3-Managed Encryption Keys (SSE-S3). Also, when using the file gateway, you can optionally configure each file share to have your objects encrypted with AWS KMS-Managed Keys using SSE-KMS. This is the reason why Option 1 is correct.

Data stored in Amazon Glacier is protected by default; only vault owners have access to the Amazon Glacier resources they create. Amazon Glacier encrypts your

data at rest by default and supports secure data transit with SSL. This is the reason why Option 4 is correct.

Options 2, 3 and 5 are because although Amazon RDS, ECS and Lambda all support encryption, you still have to enable and configure them first with tools like AWS KMS to encrypt the data at rest.

Question 22:

You run a website which accepts high-quality photos and turns them into a downloadable video montage. The website offers a free account and a premium account that guarantees faster processing. All requests by both free and premium members go through a single SQS queue and then processed by a group of EC2 instances which generate the videos. You need to ensure that the premium users who paid for the service have higher priority than your free members.

How do you re-design your architecture to address this requirement?

- **A.** For the requests made by premium members, set a higher priority in the SQS queue so it will be processed first compared to the requests made by free members.
- **B.** **Create an SQS queue for free members and another one for premium members. Configure your EC2 instances to consume messages from the premium queue first and if it is empty, poll from the free members' SQS queue. (Correct)**
- C. Use Amazon Kinesis to process the photos and generate the video montage in real time.
- D. Use Amazon S3 to store and process the photos and then generate the video montage afterwards.

EXPLANATION

In this scenario, it is best to create 2 separate SQS queues for each type of members. The SQS queues for the premium members can be polled first by the EC2 Instances and once completed, the messages from the free members can be processed next.

Option 1 is as you cannot set a priority to individual items in the SQS queue.

Option 3 is as Amazon Kinesis is used to process streaming data and it is not applicable in this scenario.

Option 4 is as Amazon S3 is used for durable storage and not for processing data.

Question 23: **In Elastic Load Balancing, there are various security features that you can use such as Server Order Preference, Predefined Security Policy,**

Perfect Forward Secrecy and many others. Perfect Forward Secrecy is a feature that provides additional safeguards against the eavesdropping of encrypted data through the use of a unique random session key. This prevents the decoding of captured data, even if the secret long-term key is compromised.

Perfect Forward Secrecy is used to offer SSL/TLS cipher suites for which two AWS services?

A. EC2 and S3
B. CloudTrail and CloudWatch
C. CloudFront and Elastic Load Balancing(Correct)
D. Trusted Advisor and GovCloud

EXPLANATION

Perfect Forward Secrecy is a feature that provides additional safeguards against the eavesdropping of encrypted data, through the use of a unique random session key. This prevents the decoding of captured data, even if the secret long-term key is compromised.

CloudFront and Elastic Load Balancing are the two AWS services that support Perfect Forward Secrecy. Hence, Option 3 is correct.

Options 1, 2, and 4 are since these services do not use Perfect Forward Secrecy. SSL/TLS is commonly used when you have sensitive data travelling through the public network.

Question 24:

One member of your DevOps team consulted you about a problem in connecting to one of the EC2 instances of your VPC over the Internet. Your environment is set up with four EC2 instances that all belong to a public subnet. The EC2 instances also belong to the same security group. Everything works well as expected except for one of the EC2 instances which is not able to send nor receive traffic over the Internet like the other three instances.

What could be the possible reason for this issue?

A. The route table is not properly configured to allow traffic to and from the Internet through the Internet gateway.
B. The EC2 instance is running in an Availability Zone that is not connected to an Internet gateway.
C. The EC2 instance does not have a private IP address associated with it.
D. The EC2 instance does not have a public IP address associated with it.(Correct)

EXPLANATION

In this scenario, there are 4 EC2 instances that belong to the same security group that should be able to connect to the Internet. The main route table is properly configured but there is a problem connecting to one instance. Since the other three instances are working fine, we can assume that the security group and the route table are correctly configured. One possible reason for this issue is that the problematic instance does not have a public or an EIP address, hence, the correct answer is Option 4.

Option 1 is because the other three instances, which are associated with the same route table and security group, do not have any issues.

Option 2 is because there is no relationship between the Availability Zone and the Internet Gateway (IGW) that may have caused the issue.

Question 25:

You have a data analytics application that updates a real-time, foreign exchange dashboard and another separate application that archives data to Amazon Redshift. Both applications are configured to consume data from the same stream concurrently and independently by using Amazon Kinesis Data Streams. However, you noticed that there are a lot of occurrences where a shard iterator expires unexpectedly. Upon checking, you found out that the DynamoDB table used by Kinesis does not have enough capacity to store the lease data.

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

- **A. Increase the write capacity assigned to the shard table.(Correct)**
- B. Upgrade the storage capacity of the DynamoDB table.
- C. Enable In-Memory Acceleration with DynamoDB Accelerator (DAX).
- D. Use Amazon Kinesis Data Analytics to properly support the data analytics application instead of Kinesis Data Stream.

EXPLANATION

A new shard iterator is returned by every GetRecords request (as NextShardIterator), which you then use in the next GetRecords request (as ShardIterator). Typically, this shard iterator does not expire before you use it. However, you may find that shard iterators expire because you have not called GetRecords for more than 5 minutes, or because you've performed a restart of your consumer application.

If the shard iterator expires immediately before you can use it, this might indicate that the DynamoDB table used by Kinesis does not have enough capacity to store the lease data. This situation is more likely to happen if you have a large number of

shards. To solve this problem, increase the write capacity assigned to the shard table. Hence, Option 1 is correct.

Option 2 is because DynamoDB is a fully managed service which automatically scales its storage, without setting it up manually. The scenario refers to the write capacity of the shard table when it says that the DynamoDB table used by Kinesis does not have enough capacity to store the lease data.

Option 3 is because the DAX feature is primarily used for read performance improvement of your DynamoDB table from milliseconds response time to microseconds. It does not have any relationship with Amazon Kinesis Data Stream in this scenario.

Option 4 is because although Amazon Kinesis Data Analytics can support a data analytics application, it is still not a suitable solution for this issue. You simply need to increase the write capacity assigned to the shard table in order to rectify the problem which is why switching to Amazon Kinesis Data Analytics is not necessary.

Question 26:

You have two On-Demand EC2 instances inside your Virtual Private Cloud in the same Availability Zone but are deployed to different subnets. One EC2 instance is running a database and the other EC2 instance a web application that connects with the database. You want to ensure that these two instances can communicate with each other for your system to work properly.

What are the things you have to check so that these EC2 instances can communicate inside the VPC?

A. **Check the Network ACL if it allows communication between the two subnets.(Correct)**
B. Check if both instances are the same instance class.
C. Check if the default route is set to a NAT instance or Internet Gateway (IGW) for them to communicate.
D. **Check if all security groups are set to allow the application host to communicate to the database on the right port and protocol.(Correct)**
E. Ensure that the EC2 instances are in the same Placement Group.

EXPLANATION

First, the Network ACL should be properly set to allow communication between the two subnets. The security group should also be properly configured so that your web server can communicate with the database server. Hence, options 1 and 4 are the correct answers:

Check if all security groups are set to allow the application host to communicate to the database on the right port and protocol.

Check the Network ACL if it allows communication between the two subnets.

Option 2 is because the EC2 instances do not need to be of the same class in order to communicate with each other.

Option 3 is because an Internet gateway is primarily used to communicate to the Internet.

Option 5 is because Placement Group is mainly used to provide low-latency network performance necessary for tightly-coupled node-to-node communication.

Question 27:

You developed a web application and deployed it on a fleet of EC2 instances, which is using Amazon SQS. The requests are saved as messages in the SQS queue which is configured with the maximum message retention period. However, after thirteen days of operation, the web application suddenly crashed and there are 10,000 unprocessed messages that are still waiting in the queue. Since you developed the application, you can easily resolve the issue but you need to send a communication to the users on the issue.

What information will you provide and what will happen to the unprocessed messages?

A. Tell the users that unfortunately, they have to resubmit all the requests again.
B. Tell the users that the application will be operational shortly however, requests sent over three days ago will need to be resubmitted.
C. Tell the users that the application will be operational shortly and all received requests will be processed after the web application is restarted. (Correct)
D. Tell the users that unfortunately, they have to resubmit all of the requests since the queue would not be able to process the 10,000 messages together.

EXPLANATION

In this scenario, it is stated that the SQS queue is configured with the maximum message retention period. The maximum message retention in SQS is 14 days that is why option 3 is the correct answer i.e. there will be no missing messages.

Options 1 and 2 are as there are no missing messages in the queue thus, there is no need to resubmit any previous requests.

Option 4 is as the queue can contain an unlimited number of messages, not just 10,000 messages.

In Amazon SQS, you can configure the message retention period to a value from 1 minute to 14 days. The default is 4 days. Once the message retention limit is reached, your messages are automatically deleted.

A single Amazon SQS message queue can contain an unlimited number of messages. However, there is a 120,000 limit for the number of inflight messages for a standard queue and 20,000 for a FIFO queue. Messages are inflight after they have been received from the queue by a consuming component, but have not yet been deleted from the queue.

Question 28:

You have started your new role as a Solutions Architect for a media company. They host large volumes of data for their operations which are about 250 TB in size on their internal servers. They have decided to store this data on S3 because of its durability and redundancy. The company currently has a 100 Mbps dedicated line connecting their head office to the Internet.

What is the fastest way to import all this data to Amazon S3?

A. Upload it directly to S3
B. Use AWS Direct connect and transfer the data over to S3.
C. Upload the files using AWS Data pipeline.
D. Use AWS Snowball to upload the files. (Correct)

EXPLANATION

Amazon Snowball is a petabyte-scale data transport solution that uses secure appliances to transfer large amounts of data into and out of the AWS cloud. Using Snowball addresses common challenges with large-scale data transfers including high network costs, long transfer times, and security concerns. Transferring data with Snowball is simple, fast, secure, and can be as little as one-fifth the cost of high-speed Internet. Hence, Option 4 is the correct answer.

Option 1 is since uploading it directly would take too long to finish.

Option 2 is since provisioning a line for Direct Connect would take too much time, and might not give you the fastest data transfer solution.

Option 3 is since Data Pipeline is a web service that makes it easy to schedule regular data movement and data processing activities in the AWS cloud. You only want a data transfer solution that is reliable, secure and fast while saving on costs.

Question 29:

You are working as a Solutions Architect for a leading commercial bank which has recently adopted a hybrid cloud architecture. You have to ensure that the required data security is in place on all of their AWS resources to meet the strict financial regulatory requirements.

In the AWS Shared Responsibility Model, which security aspects are the responsibilities of the customer?

A. Managing the underlying network infrastructure
B. Physical security of hardware
C. OS Patching of an EC2 instance(Correct)
D. IAM Policies and Credentials Management(Correct)
E. Virtualization infrastructure

EXPLANATION

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

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

The shared responsibility model for infrastructure services, such as Amazon Elastic Compute Cloud (Amazon EC2) for example, specifies that AWS manages the security of the following assets:

-Facilities

-Physical security of hardware

-Network infrastructure

-Virtualization infrastructure

You as the customer are responsible for the security of the following assets:

-Amazon Machine Images (AMIs)

-Operating systems

-Applications

-Data in transit

-Data at rest

-Data stores

-Credentials

-Policies and configuration

For a better understanding about this topic, refer to the AWS Security Best Practices whitepaper on the reference link below and also the Shared Responsibility Model diagram:

Question 30:

A corporate and investment bank has recently decided to adopt a hybrid cloud architecture for their Trade Finance web application which uses an Oracle database with Oracle Real Application Clusters (RAC) configuration. Since Oracle RAC is not supported in RDS, they decided to launch their database in a large On-Demand EC2 instance instead, with multiple EBS Volumes attached. As a Solutions Architect, you are responsible to ensure the security, availability, scalability, and disaster recovery of the whole architecture.

In this scenario, which of the following will enable you to take backups of your EBS volumes that are being used by the Oracle database?

A. EBS-backed EC2 instances.
B. Use Disk Mirroring, which is also known as RAID 1, that replicates data to two or more disks/EBS Volumes.
C. Launch the EBS Volumes to a Placement Group which will automatically back up your data.
D. Create snapshots of the EBS Volumes.(Correct)

EXPLANATION

Option 4 is correct. You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots. Snapshots are incremental backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved.

This minimizes the time required to create the snapshot and saves on storage costs by not duplicating data. When you delete a snapshot, only the data unique to that

snapshot is removed. Each snapshot contains all of the information needed to restore your data (from the moment the snapshot was taken) to a new EBS volume.

Option 1 is since running an EBS-backed EC2 instance does not relate to your problem as you are already running a few of them in the first place.

Option 2 is . Disk mirroring is not an efficient and cost-optimized solution for your problem. You should use EBS snapshots instead.

Option 3 is . A placement group is a logical grouping of instances within a single Availability Zone (AZ) that allows low-latency communication between instances. Hence, this is not an efficient way to back up data.

Question 31:

You are working as a Solutions Architect for an investment bank and your Chief Technical Officer intends to migrate all of your applications to AWS. You are looking for block storage to store all of your data and have decided to go with EBS volumes. Your boss is worried that EBS volumes are not appropriate for your workloads due to compliance requirements, downtime scenarios, and IOPS performance.

Which of the following are valid points in proving that EBS is the best service to use for your migration?

A. When you create an EBS volume in an Availability Zone, it is automatically replicated on a separate AWS region to prevent data loss due to a failure of any single hardware component.
B. EBS volumes can be attached to any EC2 Instance in any Availability Zone.
C. An EBS volume is off-instance storage that can persist independently from the life of an instance. (Correct)
D. EBS volumes support live configuration changes while in production which means that you can modify the volume type, volume size, and IOPS capacity without service interruptions. (Correct)
E. Amazon EBS provides the ability to create snapshots (backups) of any EBS volume and write a copy of the data in the volume to Amazon RDS, where it is stored redundantly in multiple Availability Zones

EXPLANATION

An Amazon EBS volume is a durable, block-level storage device that you can attach to a single EC2 instance. You can use EBS volumes as primary storage for data that requires frequent updates, such as the system drive for an instance or storage for a database application. You can also use them for throughput-intensive applications that perform continuous disk scans. EBS volumes persist independently from the running life of an EC2 instance.

Here is a list of important information about EBS Volumes:

-When you create an EBS volume in an Availability Zone, it is automatically replicated within that zone to prevent data loss due to a failure of any single hardware component.

-An EBS volume can only be attached to one EC2 instance at a time.

-After you create a volume, you can attach it to any EC2 instance in the same Availability Zone

-An EBS volume is off-instance storage that can persist independently from the life of an instance. You can specify not to terminate the EBS volume when you terminate the EC2 instance during instance creation.

-EBS volumes support live configuration changes while in production which means that you can modify the volume type, volume size, and IOPS capacity without service interruptions.

-Amazon EBS encryption uses 256-bit Advanced Encryption Standard algorithms (AES-256)

-EBS Volumes offer 99.999% SLA.

Option 1 is because when you create an EBS volume in an Availability Zone, it is automatically replicated within that zone only, and not on a separate AWS region, to prevent data loss due to a failure of any single hardware component.

Option 2 is as EBS volumes can only be attached to an EC2 instance in the same Availability Zone.

Option 5 is almost correct. But instead of storing the volume to Amazon RDS, the EBS Volume snapshots are actually sent to Amazon S3.

Question 32:

Your company has a top priority requirement to monitor a few database metrics and then afterwards, send email notifications to the Operations team in case there is an issue. Which AWS services can accomplish this requirement?

- **A.** Amazon Simple Email Service
- B. Amazon CloudWatch (Correct)
- C. Amazon Simple Queue Service (SQS)
- D. Amazon Route 53
- **E. Amazon Simple Notification Service (SNS)(Correct)**

EXPLANATION

Options 2 and 5 are correct. In this requirement, you can use Amazon CloudWatch to monitor the database and then Amazon SNS to send the emails to the Operations team. Take note that you should use SNS instead of SES (Simple Email Service) when you want to monitor your EC2 instances.

CloudWatch collects monitoring and operational data in the form of logs, metrics, and events, providing you with a unified view of AWS resources, applications, and services that run on AWS, and on-premises servers.

SNS is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications.

Option 1 is . SES is a cloud-based email sending service designed to send notification and transactional emails.

Option 3 is . SQS is a fully-managed message queuing service. It does not monitor applications nor send email notifications unlike SES.

Option 4 is . Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It does not monitor applications nor send email notifications.

Question 33:

You are a Solutions Architect of a multi-national gaming company which develops video games for PS4, Xbox One and Nintendo Switch consoles, plus a number of mobile games for Android and iOS. Due to the wide range of their products and services, you proposed that they use API Gateway.

What are the key features of API Gateway that you can tell your client?

A. It automatically provides a query language for your APIs similar to GraphQL.
B. You can run your APIs with quantum computer servers.
C. You can run your APIs without any servers.(Correct)
D. Provides durable data storage
E. You pay only for the API calls you receive and the amount of data transferred out.(Correct)

EXPLANATION

Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. With a few clicks in the AWS Management Console, you can create an API that acts as a “front door” for applications to access data, business logic, or functionality from your back-end services, such as workloads running on Amazon Elastic Compute Cloud (Amazon EC2), code running on AWS Lambda, or any web application. Since it can use AWS Lambda, you can run your APIs without servers.

Amazon API Gateway handles all the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, authorization and access control, monitoring, and API version management. Amazon API Gateway has no minimum fees or startup costs. You pay only for the API calls you receive and the amount of data transferred out.

Question 34:

A web application, which is used by your clients around the world, is hosted in an Auto Scaling group of EC2 instances behind an Application Load Balancer. You need to secure your application by allowing multiple domains to serve SSL traffic over the same IP address.

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

A. Use Server Name Indication (SNI) on your Classic Load Balancer by adding multiple SSL certificates to allow multiple domains to serve SSL traffic.
B. Generate SSL certificate with AWS Certificate Manager. Associate the certificate with your CloudFront web distribution and enable the support for Server Name Indication (SNI).(Correct)
C. Use an Elastic IP and upload multiple 3rd party certificates in your Classic Load Balancer using the AWS Certificate Manager.
D. It is not possible to allow multiple domains to serve SSL traffic over the same IP address in AWS

EXPLANATION

SNI Custom SSL relies on the SNI extension of the Transport Layer Security protocol, which allows multiple domains to serve SSL traffic over the same IP address by including the hostname which the viewers are trying to connect to.

Amazon CloudFront delivers your content from each edge location and offers the same security as the Dedicated IP Custom SSL feature. SNI Custom SSL works with most modern browsers, including Chrome version 6 and later (running on Windows XP and later or OS X 10.5.7 and later), Safari version 3 and later (running on Windows Vista and later or Mac OS X 10.5.6. and later), Firefox 2.0 and later, and Internet Explorer 7 and later (running on Windows Vista and later).

Some users may not be able to access your content because some older browsers do not support SNI and will not be able to establish a connection with CloudFront to load the HTTPS version of your content. If you need to support non-SNI compliant browsers for HTTPS content, it is recommended to use the Dedicated IP Custom SSL feature.

Option 1 is because a Classic Load Balancer does not support Server Name Indication (SNI). You have to use an Application Load Balancer instead or a CloudFront web distribution to allow the SNI feature.

Option 3 is because just like Option 1, a Classic Load Balancer does not support Server Name Indication (SNI) and the use of an Elastic IP is not a suitable solution to allow multiple domains to serve SSL traffic. You have to use Server Name Indication (SNI).

Option 4 is because AWS does support the use of Server Name Indication (SNI).

Question 35:

You have a static corporate website hosted in a standard S3 bucket and a new web domain name which was registered using Route 53. You are instructed by your manager to integrate these two services in order to successfully launch their corporate website.

What are the prerequisites when routing traffic using Amazon Route 53 to a website that is hosted in an Amazon S3 Bucket?

A. The S3 bucket name must be the same as the domain name(Correct)
B. A registered domain name(Correct)
C. The record set must be of type "MX"
D. The S3 bucket must be in the same region as the hosted zone
E. The Cross-Origin Resource Sharing (CORS) option should be enabled in the S3 bucket

EXPLANATION

Here are the prerequisites for routing traffic to a website that is hosted in an Amazon S3 Bucket:

- An S3 bucket that is configured to host a static website. The bucket must have the same name as your domain or subdomain. For example, if you want to use the subdomain portal.tutorialsdojo.com, the name of the bucket must be portal.tutorialsdojo.com.

- A registered domain name. You can use Route 53 as your domain registrar, or you can use a different registrar.

- Route 53 as the DNS service for the domain. If you register your domain name by using Route 53, we automatically configure Route 53 as the DNS service for the domain.

Option 3 is since an MX record specifies the mail server responsible for accepting email messages on behalf of a domain name. This is not what is being asked by the question.

Option 4 is . There is no constraint that the S3 bucket must be in the same region as the hosted zone, in order for the Route 53 service to route traffic into it.

Option 5 is because you only need to enable Cross-Origin Resource Sharing (CORS) when your client web application on one domain interacts with the resources in a different domain.

Question 36:

A software company has resources hosted in AWS and on-premises servers. You have been requested to create a decoupled architecture for applications which make use of both resources.

Which of the following options are valid?

- **A. Use SWF to utilize both on-premises servers and EC2 instances for your decoupled application (Correct)**
- B. Use RDS to utilize both on-premises servers and EC2 instances for your decoupled application
- **C. Use SQS to utilize both on-premises servers and EC2 instances for your decoupled application (Correct)**
- D. Use Amazon Simple Decoupling Service to utilize both on-premises servers and EC2 instances for your decoupled application
- E. Use DynamoDB to utilize both on-premises servers and EC2 instances for your decoupled application

EXPLANATION

Amazon Simple Queue Service (SQS) and Amazon Simple Workflow Service (SWF) are the services that you can use for creating a decoupled architecture in AWS. Decoupled architecture is a type of computing architecture that enables computing components or layers to execute independently while still interfacing with each other.

Amazon SQS offers reliable, highly-scalable hosted queues for storing messages while they travel between applications or microservices. Amazon SQS lets you move data between distributed application components and helps you decouple these components. Amazon SWF is a web service that makes it easy to coordinate work across distributed application components.

Options 2 and 5 are as RDS and DynamoDB are database services.

Option 4 is because there is no such thing as Amazon Simple Decoupling Service.

Question 37:

You are an AWS Network Engineer working for a utilities provider where you are managing a monolithic application with EC2 instance using a Windows AMI. You want to implement a cost-effective and highly available architecture for your application where you have an exact replica of the Windows server that is in a running state. If the primary instance terminates, you can attach the ENI to the standby secondary instance which allows the traffic flow to resume within a few seconds.

When it comes to the ENI attachment to an EC2 instance, what does 'warm attach' refer to?

- **A. Attaching an ENI to an instance when it is stopped.(Correct)**
- B. Attaching an ENI to an instance during the launch process.
- C. Attaching an ENI to an instance when it is running.
- D. Attaching an ENI to an instance when it is idle.

EXPLANATION

An elastic network interface (ENI) is a logical networking component in a VPC that represents a virtual network card. You can attach a network interface to an EC2 instance in the following ways:

When it's running (hot attach)

When it's stopped (warm attach)

When the instance is being launched (cold attach).

Therefore, option 1 is the correct answer.

Option 2 is because this describes a "cold attach" scenario.

Option 3 is because this describes a "hot attach" scenario.

Option 4 is because there is no specific name for attaching an ENI to an idle EC2 instance.

Question 38:

You have built a web application that checks for new items in an S3 bucket once every hour. If new items exist, a message is added to an SQS queue. You have a fleet of EC2 instances which retrieve messages from the SQS queue, process the file, and finally, send you and the user an email confirmation that the item has been successfully processed. Your officemate uploaded one test file to the S3 bucket and after a couple of hours, you noticed that you and your officemate have 50 emails from your application with the same message.

Which of the following is most likely the root cause why the application has sent you and the user multiple emails?

A. The sqsSendEmailMessage attribute of the SQS queue is configured to 50.
B. There is a bug in the application.
C. By default, SQS automatically deletes the messages that were processed by the consumers. It might be possible that your officemate has submitted the request 50 times which is why you received a lot of emails.
D. Your application does not issue a delete command to the SQS queue after processing the message, which is why this message went back to the queue and was processed multiple times.(Correct)

EXPLANATION

In this scenario, the main culprit is that your application does not issue a delete command to the SQS queue after processing the message, which is why this message went back to the queue and was processed multiple times.

Option 1 is as there is no sqsSendEmailMessage attribute in SQS.

Option 2 is a valid answer but since the scenario did not mention that the EC2 instances deleted the processed messages, option 4 is a better answer than this option.

Option 3 is as SQS does not automatically delete the messages.

Question 39:

You are working for a litigation firm as the Data Engineer for their case history application. You need to keep track of all the cases your firm has handled. The static assets like .jpg, .png, and .pdf files are stored in S3 for cost efficiency and high durability. As these files are critical to your business, you want to keep track of what's happening in your S3 bucket. You found out that S3 has an event notification whenever a delete or write operation happens within the S3 bucket.

What are the possible Event Notification destinations available for S3 buckets?

A. Kinesis
B. SES
C. SQS(Correct)
D. Lambda function (Correct)
E. SWF

EXPLANATION

The Amazon S3 notification feature enables you to receive notifications when certain events happen in your bucket. To enable notifications, you must first add a notification configuration identifying the events you want Amazon S3 to publish, and the destinations where you want Amazon S3 to send the event notifications.

Amazon S3 supports the following destinations where it can publish events:

Amazon Simple Notification Service (Amazon SNS) topic - A web service that coordinates and manages the delivery or sending of messages to subscribing endpoints or clients.

Amazon Simple Queue Service (Amazon SQS) queue - Offers reliable and scalable hosted queues for storing messages as they travel between computer.

AWS Lambda - AWS Lambda is a compute service where you can upload your code and the service can run the code on your behalf using the AWS infrastructure. You package up and upload your custom code to AWS Lambda when you create a Lambda function

Option 1 is because Amazon Kinesis is used to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information, and not used for event notifications. You have to use SNS, SQS or Lambda.

Option 2 is because SES is mainly used for sending emails designed to help digital marketers and application developers send marketing, notification, and transactional emails, and not for sending event notifications from S3. You have to use SNS, SQS or Lambda.

Option 5 is because SWF is mainly used to build applications that use Amazon's cloud to coordinate work across distributed components and not used as a way to trigger event notifications from S3. You have to use SNS, SQS or Lambda.

Here’s what you need to do in order to start using this new feature with your application:

Create the queue, topic, or Lambda function (which I’ll call the target for brevity) if necessary.

Grant S3 permission to publish to the target or invoke the Lambda function. For SNS or SQS, you do this by applying an appropriate policy to the topic or the queue. For Lambda, you must create and supply an IAM role, then associate it with the Lambda function.

Arrange for your application to be invoked in response to activity on the target. As you will see in a moment, you have several options here.

Set the bucket’s Notification Configuration to point to the target.

Question 40:

You have a new, dynamic web app written in MEAN stack that is going to be launched in the next month. There is a probability that the traffic will be quite high in the first couple of weeks. In the event of a load failure, how can you set up DNS failover to a static website?

A. Duplicate the exact application architecture in another region and configure DNS weight-based routing.
B. Enable failover to an application hosted in an on-premises data center.
C. Use Route 53 with the failover option to a static S3 website bucket or CloudFront distribution. (Correct)
D. Add more servers in case the application fails.

EXPLANATION

For this scenario, Option 3 is correct. You can create a new Route 53 with the failover option to a static S3 website bucket or CloudFront distribution as an alternative.

Option 1 is because running a duplicate system is not a cost-effective solution. Remember that you are trying to build a failover mechanism for your web app, not a distributed setup.

Option 2 is because, although you can set up failover to your on-premises data center, you are not maximizing the AWS environment such as using Route 53 failover.

Option 4 is because this is not the best way to handle a failover event. If you add more servers only in case the application fails, then there would be a period of downtime in which your application is unavailable. Since there are no running servers on that period, your application will be unavailable for a certain period of time until your new server is up and running.

Question 41:

As a Junior Software Engineer, you are developing a hotel reservations application and are given the task of improving the database aspect of the app. You found out that RDS does not satisfy the needs of your application because it does not scale as easily compared with DynamoDB. You need to demonstrate to your Senior Software Engineer the advantages of using DynamoDB over RDS.

What are the valid use cases for Amazon DynamoDB?

A. Running relational SQL joins and complex data updates.
B. Managing web sessions. (Correct)
C. Storing large amounts of infrequently accessed data.
D. Storing metadata for Amazon S3 objects. (Correct)
E. Storing BLOB data.

EXPLANATION

DynamoDB is a NoSQL database that supports key-value and document data structures. A key-value store is a database service that provides support for storing, querying, and updating collections of objects that are identified using a key and values that contain the actual content being stored. Meanwhile, a document data store provides support for storing, querying, and updating items in a document format such as JSON, XML, and HTML.

Option 2 is correct because the DynamoDB Time-to-Live (TTL) mechanism enables you to manage web sessions of your application easily. It lets you set a specific timestamp to delete expired items from your tables. Once the timestamp expires, the corresponding item is marked as expired and is subsequently deleted from the table. By using this functionality, you do not have to track expired data and delete it manually. TTL can help you reduce storage usage and reduce the cost of storing data that is no longer relevant.

Option 4 is correct because the Amazon DynamoDB stores structured data indexed by primary key and allow low latency read and write access to items ranging from 1 byte up to 400KB. Amazon S3 stores unstructured blobs and is suited for storing large objects up to 5 TB. In order to optimize your costs across AWS services, large objects or infrequently accessed data sets should be stored in Amazon S3, while smaller data elements or file pointers (possibly to Amazon S3 objects) are best saved in Amazon DynamoDB.

To speed up access to relevant data, you can pair Amazon S3 with a search engine such as Amazon CloudSearch or a database such as Amazon DynamoDB or Amazon RDS. In these scenarios, Amazon S3 stores the actual information, and the search engine or database serves as the repository for associated metadata such as the object name, size, keywords, and so on. Metadata in the database can easily be indexed and queried, making it very efficient to locate an object's reference by using a search engine or a database query. This result can be used to pinpoint and retrieve the object itself from Amazon S3.

Option 1 is since DynamoDB is a NoSQL database solution and not a relational database.

Option 3 is because DynamoDB is not meant to store large amounts of infrequently accessed data, due to factors like sizing, scaling and cost. Amazon Glacier would be a better option for this scenario.

Option 5 is because BLOB data is too large a chunk of data to be put into a NoSQL database such as DynamoDB.

Question 42:

You are working for a large telecommunications company. They have a requirement to move 83 TB data warehouse to the cloud. It would take 2 months to transfer the data given their current bandwidth allocation.

Which is the most cost-effective service that would allow you to quickly upload their data into AWS?

A. Amazon Snowball
B. Amazon Snowball Edge (Correct)
C. Amazon Direct Connect
D. Amazon S3 MultiPart Upload

EXPLANATION

Although an AWS Snowball device costs less than AWS Snowball Edge, it cannot store 80 TB of data in one device. Take note that the storage capacity is different from the usable capacity for Snowball and Snowball Edge. Remember that an 80 TB Snowball appliance and 100 TB Snowball Edge appliance only have 72 TB and 83 TB of usable capacity respectively. Hence, it would be costly if you use two Snowball devices compared to using just one AWS Snowball Edge device.

The AWS Snowball Edge is a type of Snowball device with on-board storage and compute power for select AWS capabilities. Snowball Edge can undertake local processing and edge-computing workloads in addition to transferring data between your local environment and the AWS Cloud.

Each Snowball Edge device can transport data at speeds faster than the internet. This transport is done by shipping the data in the appliances through a regional carrier. The appliances are rugged shipping containers, complete with E Ink shipping labels. The AWS Snowball Edge device differs from the standard Snowball because it can bring the power of the AWS Cloud to your on-premises location, with local storage and compute functionality.

Snowball Edge devices have three options for device configurations – storage optimized, compute optimized, and with GPU. When this guide refers to Snowball Edge devices, it's referring to all options of the device. Whenever specific information applies only to one or more optional configurations of devices, like how the Snowball Edge with GPU has an on-board GPU, it will be called out.

Question 43:

You work for an Intelligence Agency as its Principal Consultant developing a missile tracking application, which is hosted on both development and production AWS accounts. Alice, the Intelligence agency's Junior Developer,

only has access to the development account. She has received security clearance to access the agency's production account but the access is only temporary and only write access to EC2 and S3 is allowed.

Which of the following allows you to issue short-lived access tokens that acts as temporary security credentials to allow access to your AWS resources?

A. Use AWS Cognito to issue JSON Web Tokens (JWT)
B. Use AWS STS(Correct)
C. Use AWS SSO
D. All of the above.

EXPLANATION

AWS Security Token Service (AWS STS) is the service that you can use to create and provide trusted users with temporary security credentials that can control access to your AWS resources. Temporary security credentials work almost identically to the long-term access key credentials that your IAM users can use.

In this diagram, IAM user Alice in the Dev account (the role-assuming account) needs to access the Prod account (the role-owning account). Here's how it works:

Alice in the Dev account assumes an IAM role (WriteAccess) in the Prod account by calling AssumeRole.

STS returns a set of temporary security credentials.

Alice uses the temporary security credentials to access services and resources in the Prod account. Alice could, for example, make calls to Amazon S3 and Amazon EC2, which are granted by the WriteAccess role.

Option 1 is because the Amazon Cognito service is primarily used for user authentication and not for providing access to your AWS resources. A JSON Web Token (JWT) is meant to be used for user authentication and session management.

Option 3 is because although the AWS SSO service uses STS, it does not issue short-lived credentials by itself. AWS Single Sign-On (SSO) is a cloud SSO service that makes it easy to centrally manage SSO access to multiple AWS accounts and business applications.

Option 4 is as only STS has the ability to provide temporary security credentials.

Question 44:

As part of the Business Continuity Plan of your company, your IT Director instructed you to set up an automated backup of all of the EBS Volumes for your EC2 instances as soon as possible.

What is the fastest and most cost-effective solution to automatically back up all of your EBS Volumes?

A. For an automated solution, create a scheduled job that calls the "create-snapshot" command via the AWS CLI to take a snapshot of production EBS volumes periodically.
B. Set your Amazon Storage Gateway with EBS volumes as the data source and store the backups in your on-premises servers through the storage gateway.
C. Use an EBS-cycle policy in Amazon S3 to automatically back up the EBS volumes.
D. Use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation of EBS snapshots. (Correct)

EXPLANATION

You can use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation, retention, and deletion of snapshots taken to back up your Amazon EBS volumes. Automating snapshot management helps you to:

-Protect valuable data by enforcing a regular backup schedule.

-Retain backups as required by auditors or internal compliance.

-Reduce storage costs by deleting outdated backups.

Combined with the monitoring features of Amazon CloudWatch Events and AWS CloudTrail, Amazon DLM provides a complete backup solution for EBS volumes at no additional cost. Hence, Option 5 is the correct answer as it is the fastest and cost-effective solution in providing an automated way of backing up your EBS volumes.

Option 1 is because even though this is a valid solution, you would still need additional time to create a scheduled job that calls the "create-snapshot" command. It would be better to use Amazon Data Lifecycle Manager (Amazon DLM) instead as this provides you the fastest solution which enables you to automate the creation, retention, and deletion of the EBS snapshots without having to write custom shell scripts or creating scheduled jobs.

Option 2 is as the Amazon Storage Gateway is used only for creating a backup of data from your on-premises server and not from the Amazon Virtual Private Cloud.

Option 3 is as there is no such thing as EBS-cycle policy in Amazon S3.

Question 45:

You are working for a commercial bank as an AWS Infrastructure Engineer handling the forex trading application of the bank. You have an Auto Scaling group of EC2 instances that allow your company to cope up with the current demand of traffic and achieve cost-efficiency. You want the Auto Scaling group to behave in such a way that it will follow a predefined set of parameters before it scales down the number of EC2 instances, which protects your system from unintended slowdown or unavailability.

Which of the following statements are true regarding the cooldown period?

A. It ensures that before the Auto Scaling group scales out, the EC2 instances have an ample time to cooldown.
B. It ensures that the Auto Scaling group launches or terminates additional EC2 instances without any downtime.
C. It ensures that the Auto Scaling group does not launch or terminate additional EC2 instances before the previous scaling activity takes effect.(Correct)
D. Its default value is 300 seconds.(Correct)
E. Its default value is 600 seconds.

EXPLANATION

In Auto Scaling, the following statements are correct regarding the cooldown period:

It ensures that the Auto Scaling group does not launch or terminate additional EC2 instances before the previous scaling activity takes effect.

Its default value is 300 seconds.

It is a configurable setting for your Auto Scaling group.

Options 1, 2, and 5 are as these statements are false in depicting what the word "cooldown" actually means for Auto Scaling. The cooldown period is a configurable setting for your Auto Scaling group that helps to ensure that it doesn't launch or terminate additional instances before the previous scaling activity takes effect. After the Auto Scaling group dynamically scales using a simple scaling policy, it waits for the cooldown period to complete before resuming scaling activities.

Question 46:

You are a Solutions Architect of a media company and you are instructed to migrate an on-premises web application architecture to AWS. During your design process, you have to give consideration to current on-premises security and determine which security attributes you are responsible for on AWS.

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

A. Customer Data
B. Physical network infrastructure (Correct)
C. Instance security
D. User access to the AWS environment

EXPLANATION

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

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

Option 1 is since providing you customer data would be a breach in security protocols and data privacy laws.

Option 3 is because it is your responsibility to set up the security tools AWS has provided you to secure your instances in your cloud environment.

Option 4 is since it is your responsibility to delegate user access to your cloud environment.

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

Question 47:

To protect your enterprise applications against unauthorized access, you configured multiple rules for your Network ACLs in your VPC. How are the access rules evaluated?

A. Network ACL Rules are evaluated by rule number, from highest to lowest and are executed immediately when a matching allow/deny rule is found.
B. By default, all Network ACL Rules are evaluated before any traffic is allowed or denied.
C. Network ACL Rules are evaluated by rule number, from lowest to highest, and executed immediately when a matching allow/deny rule is found. (Correct)
D. Network ACL Rules are evaluated by rule number, from lowest to highest, and executed after all rules are checked for conflicting allow/deny rules.

EXPLANATION

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

Network ACL Rules are evaluated by rule number, from lowest to highest, and executed immediately when a matching allow/deny rule is found.

Option 1 is since rules are evaluated from lowest to highest, not the other way around.

Option 2 is because the Network ACL Rules are evaluated by rule number, from lowest to highest, and executed immediately when a matching allow/deny rule is found.

Option 4 is since rules are executed immediately when a match is found and not after all rules are checked for conflicting allow/deny rules.

Question 48:

Using the EC2 API, you requested 40 m5.large On-Demand EC2 instances in a single Availability Zone. Twenty instances were successfully created but the other 20 requests failed.

What is the solution for this issue and what is the root cause?

A. **For new accounts, there is a soft limit of 20 EC2 instances per region. Submit an Amazon EC2 instance Request Form in order to lift this limit. (Correct)**
B. You can only create 20 instances per Availability Zone. Select a different Availability Zone and retry creating the instances again.
C. A certain Inbound Rule in your Network Access List is preventing you to create more than 20 instances. Remove this rule and the issue will be resolved.
D. The API credentials that you are using has a limit of only 20 requests per hour. Try submitting the request again after one hour.

EXPLANATION

Amazon EC2 has a soft limit of 20 instances per region, which can be easily resolved by completing the Amazon EC2 instance request form where your use case and your instance increase will be considered. Limit increases are tied to the region they were requested for.

Option 2 is as there is no such limit in the Availability Zone.

Option 3 is . Network Access List is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. It does not affect the creation of new EC2 instances.

Option 4 is as there is no problem with your API credentials.

Question 49:

You work for a brokerage firm as an AWS Infrastructure Engineer who handles the stocks trading application. You host your database in an EC2 server with two EBS volumes for OS and data storage in ap-southeast-1a. Due to the fault tolerance requirements, there is a need to assess if the EBS volumes will be affected in the event of ap-southeast-1a availability zone outage.

Can EBS tolerate an Availability Zone failure each and every time?

A. **No, all EBS volumes are stored and replicated in a single AZ only.(Correct)**
B. Yes, EBS volume is fault-tolerant and has multiple copies across multiple AZ.
C. Depends on how the EBS volume is set up.
D. Depends on the AWS region where the EBS volume is created.

EXPLANATION:

Option 1 is correct because when you create an EBS volume in an Availability Zone, it is automatically replicated within that zone only to prevent data loss due to a failure of any single hardware component. After you create a volume, you can attach it to any EC2 instance in the same Availability Zone.

Option 2 is because it is the EBS snapshots, not the EBS volume, that has a copy of the data which is stored redundantly in multiple Availability Zones.

Option 3 is because there is no option to span an EBS volume in different availability zones.

Option 4 is because it doesn't matter which AWS region the EBS volume is created. EBS volumes only exist in a single availability zone while EBS snapshots are available in one AWS region.

Question 50:

Your client is an insurance company that utilizes SAP HANA for their day-to-day ERP operations. Since you can't migrate this database due to customer preferences, you need to integrate it with your current AWS workload in your VPC in which you are required to establish a site-to-site VPN connection.

What needs to be configured outside of the VPC for you to have a successful site-to-site VPN connection?

A. A dedicated NAT instance in a public subnet
B. An Internet-routable IP address (static) of the customer gateway's external interface for the on-premises network. (Correct)
C. The main route table in your VPC to route traffic through a NAT instance
D. An EIP to the Virtual Private Gateway

EXPLANATION:

By default, instances that you launch into a virtual private cloud (VPC) can't communicate with your own network. You can enable access to your network from your VPC by attaching a virtual private gateway to the VPC, creating a custom route table, updating your security group rules, and creating an AWS managed VPN connection.

Although the term VPN connection is a general term, in the Amazon VPC documentation, a VPN connection refers to the connection between your VPC and your own network. AWS supports Internet Protocol security (IPsec) VPN connections.

A customer gateway is a physical device or software application on your side of the VPN connection.

To create a VPN connection, you must create a customer gateway resource in AWS, which provides information to AWS about your customer gateway device. Next, you have to set up an Internet-routable IP address (static) of the customer gateway's external interface.

The following diagram illustrates single VPN connections. The VPC has an attached virtual private gateway, and your remote network includes a customer gateway, which you must configure to enable the VPN connection. You set up the routing so that any traffic from the VPC bound for your network is routed to the virtual private gateway.

Options 1 and 3 are since you don't need a NAT instance for you to be able to create a VPN connection.

Option 4 is since you do not attach an EIP to a VPG.

Question 51:

Your company is running a multi-tier web application farm in a virtual private cloud (VPC) that is not connected to their corporate network. They are connecting to the VPC over the Internet to manage the fleet of Amazon EC2 instances running in both the public and private subnets. You have added a bastion host with Microsoft Remote Desktop Protocol (RDP) access to the application instance security groups, but the company wants to further limit administrative access to all of the instances in the VPC.

Which of the following bastion host deployment options will meet this requirement?

A. Deploy a Windows Bastion host on the corporate network that has RDP access to all EC2 instances in the VPC.
B. Deploy a Windows Bastion host with an Elastic IP address in the private subnet, and restrict RDP access to the bastion from only the corporate public IP addresses.
C. Deploy a Windows Bastion host with an Elastic IP address in the public subnet and allow SSH access to the bastion from anywhere.
D. Deploy a Windows Bastion host with an Elastic IP address in the public subnet and allow RDP access to bastion only from the corporate IP addresses.(Correct)

EXPLANATION

The correct answer is to deploy a Windows Bastion host with an Elastic IP address in the public subnet and allow RDP access to bastion only from the corporate IP addresses.

A bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks. If you have a bastion host in AWS, it is basically just an EC2 instance. It should be in a public subnet with either a public or Elastic IP address with sufficient RDP or SSH access defined in the security group. Users log on to the bastion host via SSH or RDP and then use that session to manage other hosts in the private subnets.

Option 1 is since you do not deploy the Bastion host to your corporate network. It should be in the public subnet of a VPC.

Option 2 is since it should be deployed in a public subnet, not a private subnet.

Option 3 is . Since it is a Windows bastion, you should allow RDP access and not SSH as this is mainly used for Linux-based systems.

Question 52:

For data privacy, a healthcare company has been asked to comply with the Health Insurance Portability and Accountability Act (HIPAA). They have been told that all of the data being backed up or stored on Amazon S3 must be encrypted.

What is the best option to do this?

A. Before sending the data to Amazon S3 over HTTPS, encrypt the data locally first using your own encryption keys.(Correct)

B. Store the data on EBS volumes with encryption enabled instead of using Amazon S3.
C. Store the data in encrypted EBS snapshots.
D. Enable Server-Side Encryption on an S3 bucket to make use of AES-256 encryption.(Correct)
E. Enable Server-Side Encryption on an S3 bucket to make use of AES-128 encryption.

EXPLANATION

Server-side encryption is about data encryption at rest—that is, Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects. For example, if you share your objects using a pre-signed URL, that URL works the same way for both encrypted and unencrypted objects.

You have three mutually exclusive options depending on how you choose to manage the encryption keys:

Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Use Server-Side Encryption with Customer-Provided Keys (SSE-C)

Options 1 and 4 are correct because they are using Amazon S3-Managed Keys (SSE-S3) and Customer-Provided Keys (SSE-C). SSE-S3 uses AES-256 encryption and SSE-C allows you to use your own encryption key.

Options 2 and 3 are because both options use EBS encryption and not S3.

Option 5 is as S3 doesn't provide AES-128 encryption, only AES-256.

Question 53:

You are working for an online hotel booking firm with terabytes of customer data coming from your websites and applications. There is an annual corporate meeting where you need to present the booking behavior and acquire new insights from your customers' data. You are looking for a service to perform super-fast analytics on massive data sets in near real-time.

Which of the following services gives you the ability to store huge amounts of data and perform quick and flexible queries on it?

A. DynamoDB
B. ElastiCache
C. RDS
D. Redshift(Correct)

EXPLANATION

Amazon Redshift is a fast, scalable data warehouse that makes it simple and cost-effective to analyze all your data across your data warehouse and data lake. Redshift delivers ten times faster performance than other data warehouses by using machine learning, massively parallel query execution, and columnar storage on high-performance disk.

Option 1 is . DynamoDB is a NoSQL database which is based on key-value pairs used for fast processing of small data that dynamically grows and changes. But if you need to scan large amounts of data (ie a lot of keys all in one query), the performance will not be optimal.

Option 2 is because Elasticache is used to increase the performance, speed and redundancy with which applications can retrieve data by providing an in-memory database caching system, and not for database analytical processes.

Option 3 is because RDS is mainly used for On-Line Transaction Processing (OLTP) applications and not for Online Analytics Processing (OLAP).

Question 54:

You have set up a VPC with public subnet and an Internet gateway. You set up an EC2 instance with a public IP as well. However, you are still not able to connect to the instance via the Internet. You checked its associated security group and it seems okay.

What should you do to ensure you can connect to the EC2 instance from the Internet?

A. Set an Elastic IP Address to the EC2 instance.
B. Set a Secondary Private IP Address to the EC2 instance.
C. Check the main route table and ensure that the right route entry to the Internet Gateway (IGW) is configured. (Correct)
D. Check the CloudWatch logs as there must be some issue in the EC2 instance.

EXPLANATION

The route table entries enable EC2 instances in the subnet to use IPv4 to communicate with other instances in the VPC, and to communicate directly over the Internet. A subnet that's associated with a route table that has a route to an Internet gateway is known as a public subnet.

If you could not connect to your EC2 instance even if there is already an Internet Gateway in your VPC and there is no issue in the security group, then you must check if the entries in the route table are properly configured.

Option 1 is since you already have a public IP address for your EC2 instance, and doesn't require an EIP anymore.

Option 2 is because having a secondary private IP address is only used within the VPC, not when connecting to the outside Internet.

Option 4 is because it is better to go through your setup and make sure that you didn't miss a step, such as adding a route in the route table, before you check the actual CloudWatch logs to see if an instance has an issue.

Question 55:

You are working for an advertising company as their Senior Solutions Architect handling the S3 storage data. Your company has terabytes of data sitting on AWS S3 standard storage class, which accumulates significant operational costs. The management wants to cut down on the cost of their cloud infrastructure so you were instructed to switch to Glacier to lessen the cost per GB storage.

The Amazon Glacier storage service is primarily used for which use case?

A. Storing cached session data
B. Storing infrequently accessed data(Correct)
C. Storing Data archives(Correct)
D. Used for active database storage
E. Used as a data warehouse

EXPLANATION

Amazon Glacier is an extremely low-cost storage service that provides secure, durable, and flexible storage for data backup and archival. Amazon Glacier is designed to store data that is infrequently accessed. Amazon Glacier enables customers to offload the administrative burdens of operating and scaling storage to AWS so that they don’t have to worry about capacity planning, hardware provisioning, data replication, hardware failure detection and repair, or time-consuming hardware migrations.

Option 1 is because storing cached session data is the main use case for ElastiCache and not Amazon Glacier.

Option 4 is because you should use RDS or DynamoDB for your active database storage as S3, in general, is used for storing your data or files.

Option 5 is because storing it for data warehousing is the main use case of Amazon Redshift. It does not meet the requirement of being able to archive your infrequently accessed data. You can use S3 standard instead for frequently accessed data or Glacier for infrequently accessed data and archiving.

It is advisable to transition the standard data to infrequent access first then transition it to Amazon Glacier. You can specify in the lifecycle rule the time it will sit in standard tier and infrequent access. You can also delete the objects after a certain amount of time.

In transitioning S3 standard to Glacier you need to tell S3 which objects are to be archived to the new Glacier storage option, and under what conditions. You do this by setting up a lifecycle rule using the following elements:

-A prefix to specify which objects in the bucket are subject to the policy.

-A relative or absolute time specifier and a time period for transitioning objects to Glacier. The time periods are interpreted with respect to the object's creation date. They can be relative (migrate items that are older than a certain number of days) or absolute (migrate items on a specific date)

-An object age at which the object will be deleted from S3. This is measured from the original PUT of the object into the service, and the clock is not reset by a transition to Glacier.

You can create a lifecycle rule in the AWS Management Console.

Question 56:

You are working for a University as their AWS Consultant. They want to have a disaster recovery strategy in AWS for mission-critical applications after suffering a disastrous outage wherein they lost student and employee records. They don't want this to happen again but at the same time want to minimize the monthly costs. You are instructed to set up a minimum version of the application that is always available in case of any outages.

Which of the following disaster recovery architectures is the most suitable one to use in this scenario?

A. Backup & Restore
B. Pilot Light(Correct)
C. Warm Standby
D. Multi Site

EXPLANATION

The correct answer is option 2 - Pilot Light.

The term pilot light is often used to describe a DR scenario in which a minimal version of an environment is always running in the cloud. The idea of the pilot light is an analogy that comes from the gas heater. In a gas heater, a small flame that's always on can quickly ignite the entire furnace to heat up a house. This scenario is similar to a backup-and-restore scenario.

For example, with AWS you can maintain a pilot light by configuring and running the most critical core elements of your system in AWS. When the time comes for recovery, you can rapidly provision a full-scale production environment around the critical core.

Option 1 is because you are running mission-critical applications, and the speed of recovery from backup and restore solution might not meet your RTO and RPO.

Option 3 is . Warm standby is a method of redundancy in which the scaled-down secondary system runs in the background of the primary system. Doing so would not optimize your savings as much as running a pilot light recovery since some of your services are always running in the background.

Option 4 is as well. Multi-site is the most expensive solution out of disaster recovery solutions. You are trying to save monthly costs so this should be the least probable choice for you.

Question 57:

A start-up company has an EC2 instance that is hosting a web application. The volume of users is expected to grow in the coming months and hence, you need to add more elasticity and scalability in your AWS architecture to cope with the demand.

Which of the following options can satisfy the above requirement for the given scenario?

A. Set up two EC2 instances and then put them behind an Elastic Load balancer (ELB).(Correct)
B. Set up an S3 Cache in front of the EC2 instance.
C. Set up two EC2 instances and use Route 53 to route traffic based on a Weighted Routing Policy.(Correct)
D. Set up an AWS WAF behind your EC2 Instance.
E. Set up two EC2 instances deployed using Launch Templates and integrated with AWS Glue.

EXPLANATION

Using an Elastic Load Balancer is an ideal solution for adding elasticity to your application. Alternatively, you can also create a policy in Route53, such as a Weighted routing policy, to evenly distribute the traffic to 2 or more EC2 instances. Hence Options 1 and 3 are the correct answers.

Option 2 is because setting up an S3 cache does not provide elasticity and scalability to your EC2 instances.

Option 4 is because AWS WAF is a web application firewall that helps protect your web applications from common web exploits. This service is more on providing security to your applications.

Option 5 is because AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. It does not provide scalability or elasticity to your instances.

Question 58:

An accounting application uses an RDS database configured with Multi-AZ deployments to improve availability. What would happen to RDS if the primary database instance fails?

A. The IP address of the primary DB instance is switched to the standby DB instance.
B. The primary database instance will reboot.
C. A new database instance is created in the standby Availability Zone.
D. The canonical name record (CNAME) is switched from the primary to standby instance. (Correct)

EXPLANATION

In Amazon RDS, failover is automatically handled so that you can resume database operations as quickly as possible without administrative intervention in the event that your primary database instance went down. When failing over, Amazon RDS simply flips the canonical name record (CNAME) for your DB instance to point at the standby, which is in turn promoted to become the new primary.

Option 1 is since IP addresses are per subnet, and subnets cannot span multiple AZs.

Option 2 is since in the event of a failure, there is no database to reboot with.

Option 3 is since with multi-AZ enabled, you already have a standby database in another AZ.

Question 59:

You are a Solutions Architect working for a large insurance company that deployed their production environment on a custom Virtual Private Cloud in AWS with a default configuration. The VPC consists of two private subnets

and one public subnet. Inside the public subnet is a group of EC2 instances which are created by an Auto Scaling group and all of the instances are in the same Security Group. Your development team has created a new web application which connects to mobile devices using a custom port. This application has been deployed to the production environment and you need to open this port globally to the Internet.

Which of the following is the correct procedure?

A. Open the custom port on the Security Group. Your EC2 instances will be able to use this port after 60 minutes.
B. Open the custom port on the Network Access Control List of your VPC. Your EC2 instances will be able to use this port immediately.
C. Open the custom port on the Security Group. Your EC2 instances will be able to use this port immediately.(Correct)
D. Open the custom port on the Network Access Control List of your VPC. Your EC2 instances will be able to use this port after a reboot.

EXPLANATION

To allow the custom port, you have to change the Inbound Rules in your Security Group to allow traffic coming from the mobile devices. Security Groups usually control the list of ports that are allowed to be used by your EC2 instances and the NACLs control which network or list of IP addresses can connect to your whole VPC.

When you create a security group, it has no inbound rules. Therefore, no inbound traffic originating from another host to your instance is allowed until you add inbound rules to the security group. By default, a security group includes an outbound rule that allows all outbound traffic. You can remove the rule and add outbound rules that allow specific outbound traffic only. If your security group has no outbound rules, no outbound traffic originating from your instance is allowed.

Options 1 and 4 are both because any changes to the Security Groups or Network Access Control Lists are applied immediately and not after 60 minutes or after the instance reboot.

Option 2 is because the scenario says that VPC is using a default configuration. Since by default, Network ACL allows all inbound and outbound IPv4 traffic, then there is no point of explicitly allowing the port in the Network ACL. Security Groups, on the other hand, does not allow incoming traffic by default, unlike Network ACL.

Question 60:

You are helping out a new DevOps Engineer to design her first architecture in AWS. She is planning to develop a highly available and fault-tolerant architecture which is composed of an Elastic Load Balancer and an Auto Scaling group of EC2 instances deployed across multiple Availability Zones. This will be used by an online accounting application which requires TLS

termination capabilities, path-based routing, host-based routing, and bi-directional communication channels using WebSockets.

Which is the most suitable type of Elastic Load Balancer that you should recommend for her to use?

- **A. Application Load Balancer(Correct)**
- B. Network Load Balancer
- C. Classic Load Balancer
- D. Either a Classic Load Balancer or a Network Load Balancer

EXPLANATION

Elastic Load Balancing supports three types of load balancers. You can select the appropriate load balancer based on your application needs.

If you need flexible application management and TLS termination then we recommend that you use Application Load Balancer. If extreme performance and static IP is needed for your application then we recommend that you use Network Load Balancer. If your application is built within the EC2 Classic network then you should use Classic Load Balancer.

An Application Load Balancer functions at the application layer, the seventh layer of the Open Systems Interconnection (OSI) model. After the load balancer receives a request, it evaluates the listener rules in priority order to determine which rule to apply, and then selects a target from the target group for the rule action. You can configure listener rules to route requests to different target groups based on the content of the application traffic. Routing is performed independently for each target group, even when a target is registered with multiple target groups.

Application Load Balancers support TLS termination capabilities, path-based routing, host-based routing and support for containerized applications hence, Option 1 is correct.

Options 2, 3 and 4 are as none of these support path-based routing and host-based routing, unlike an Application Load Balancer.

Question 61:

A start-up company that offers an intuitive financial data analytics service has consulted you about their AWS architecture. They have a fleet of Amazon EC2 worker instances that process financial data and then outputs reports which are used by their clients. You must store the generated report files in a durable storage. The number of files to be stored can grow over time as the start-up company is expanding rapidly overseas and hence, they also need a way to distribute the reports faster to clients located across the globe.

Which of the following is a cost-efficient and scalable storage option that you should use for this scenario?

A. Use Amazon Redshift as the data storage and CloudFront as the CDN.
B. Use Amazon Glacier as the data storage and ElastiCache as the CDN.
C. Use Amazon S3 as the data storage and CloudFront as the CDN.(Correct)
D. Use multiple EC2 instance stores for data storage and ElastiCache as the CDN.

EXPLANATION

Amazon S3 offers a highly durable, scalable, and secure destination for backing up and archiving your critical data. This is the correct option as the start-up company is looking for a durable storage to store the audio and text files. In addition, ElastiCache is only used for caching and not specifically as a Global Content Delivery Network (CDN).

Option 1 is as Amazon Redshift is usually used as a Data Warehouse.

Option 2 is as Amazon Glacier is usually used for data archives.

Option 4 is as data stored in an instance store is not durable.

Question 62:

You are an IT Consultant for an advertising company that is currently working on a proof of concept project that automatically provides SEO analytics for their clients. Your company has a VPC in AWS that operates in dual-stack mode in which IPv4 and IPv6 communication is allowed. You deployed the application to an Auto Scaling group of EC2 instances with an Application Load Balancer in front that evenly distributes the incoming traffic. You are ready to go live but you need to point your domain name (tutorialsdojo.com) to the Application Load Balancer.

In Route 53, which record types will you use to point the DNS name of the Application Load Balancer?

A. Non-Alias with a type "A" record set
B. Alias with a type "AAAA" record set(Correct)
C. Alias with a type "CNAME" record set
D. Alias with a type "A" record set(Correct)
E. Alias with a type of “MX” record set

EXPLANATION

Options 2 and 4 are correct. To route domain traffic to an ELB load balancer, use Amazon Route 53 to create an alias record that points to your load balancer. An alias record is a Route 53 extension to DNS. It's similar to a CNAME record, but you can create an alias record both for the root domain, such as tutorialsdojo.com, and for subdomains, such as portal.tutorialsdojo.com. (You can create CNAME records only for subdomains.) To enable IPv6 resolution, you would need to create a second resource record, tutorialsdojo.com ALIAS AAAA -> myelb.us-west-2.elb.amazonnaws.com, this is assuming your Elastic Load Balancer has IPv6 support.

Option 1 is because you only use Non-Alias with a type “A” record set for IP addresses.

Option 3 is because you can't create a CNAME record at the zone apex. For example, if you register the DNS name tutorialsdojo.com, the zone apex is tutorialsdojo.com.

Option 5 is because an MX record is primarily used for mail servers. It includes a priority number and a domain name, for example, 10 mailserver.tutorialsdojo.com.

Question 63:

A San Francisco-based tech startup is building a cross-platform mobile app that can notify the user with upcoming astronomical events such as eclipses, blue moon, novae or a meteor shower. Your mobile app authenticates with the Identity Provider (IdP) using the provider's SDK and Amazon Cognito. Once the end user is authenticated with the IdP, the OAuth or OpenID Connect token returned from the IdP is passed by your app to Amazon Cognito.

Which of the following is returned for the user to provide a set of temporary, limited-privilege AWS credentials?

A. Cognito SDK
B. Cognito Key Pair
C. Cognito ID(Correct)
D. Cognito API

EXPLANATION

You can use Amazon Cognito to deliver temporary, limited-privilege credentials to your application so that your users can access AWS resources. Amazon Cognito identity pools support both authenticated and unauthenticated identities. You can retrieve a unique Amazon Cognito identifier (identity ID) for your end user immediately if you're allowing unauthenticated users or after you've set the login tokens in the credentials provider if you're authenticating users.

That is why the correct answer for this question is Option 3: Cognito ID.

Option 1 is because Cognito SDK is not the unique Amazon Cognito identifier but a software development kit that is available in various programming languages.

Option 2 is because Cognito Key Pair is not the unique Amazon Cognito identifier but a cryptography key.

Option 4 is because the Cognito API is not the unique Amazon Cognito identifier and is primarily used as an Application Programming Interface.

Question 64:

Your customer is building an internal application that serves as a repository for images uploaded by a couple of users. Whenever a user uploads an image, it would be sent to Kinesis for processing before it is stored in an S3 bucket. Afterwards, if the upload was successful, the application will return a prompt telling the user that the upload is successful. The entire processing typically takes about 5 minutes to finish.

Which of the following options will allow you to asynchronously process the request to the application in the most cost-effective manner?

A. Use a combination of Lambda and Step Functions to orchestrate service components and asynchronously process the requests.
B. Use a combination of a Lambda function and SQS to queue the requests and then asynchronously process them by using Lambda.
C. **Create a Lambda function that will asynchronously process the requests.(Correct**)
D. Use a combination of a Lambda function and SNS to asynchronously process the requests by sending a notification back to Lambda once the image has been successfully processed.

EXPLANATION

AWS Lambda supports synchronous and asynchronous invocation of a Lambda function. You can control the invocation type only when you invoke a Lambda function. When you use an AWS services as a trigger, the invocation type is predetermined for each service. You have no control over the invocation type that these event sources use when they invoke your Lambda function. Since the processing only takes 5 minutes, Lambda is also a cost-effective choice.

Option 1 is because the AWS Step Functions service lets you coordinate multiple AWS services into serverless workflows so you can build and update apps quickly. Although this can be a valid solution, it is not cost-effective since the application does not have a lot of components to orchestrate. Lambda functions can effectively meet the requirements in this scenario without using Step Functions. This service is not as cost-effective as Lambda.

Options 2 and 4 are as SQS and SNS are messaging services and do not perform asynchronous function calls.

Question 65:

You have a cryptocurrency exchange portal which is hosted in an Auto Scaling group of EC2 instances behind an Application Load Balancer, and are deployed across multiple AWS regions. Your users can be found all around the globe, but the majority are from Japan and Sweden. Because of the compliance requirements in these two locations, you want your Japanese users to connect to the servers in the ap-northeast-1 Asia Pacific (Tokyo) region, while your Swedish users should be connected to the servers in the eu-west-1 EU (Ireland) region.

Which of the following services would allow you to easily fulfill this requirement?

- **A. Use Route 53 Geolocation Routing policy.(Correct)**
- B. Set up an Application Load Balancers that will automatically route the traffic to the proper AWS region.
- C. Set up a new CloudFront web distribution with the geo-restriction feature enabled.
- D. Use Route 53 Weighted Routing policy.

EXPLANATION

Geolocation routing lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location that DNS queries originate from. For example, you might want all queries from Europe to be routed to an ELB load balancer in the Frankfurt region.

When you use geolocation routing, you can localize your content and present some or all of your website in the language of your users. You can also use geolocation routing to restrict distribution of content to only the locations in which you have distribution rights. Another possible use is for balancing load across endpoints in a predictable, easy-to-manage way, so that each user location is consistently routed to the same endpoint.

Option 2 is because Elastic Load Balancers distribute traffic among EC2 instances across multiple Availability Zones but not across AWS regions.

Option 3 is because the CloudFront geo-restriction feature is primarily used to prevent users in specific geographic locations from accessing content that you're distributing through a CloudFront web distribution. It does not let you choose the resources that serve your traffic based on the geographic location of your users, unlike the Geolocation routing policy in Route 53.

Option 4 is because the Route 53 Weighted Routing policy is not a suitable solution to meet the requirements of this scenario. It just lets you associate multiple resources with a single domain name (tutorialsdojo.com) or subdomain name (forums.tutorialsdojo.com) and choose how much traffic is routed to each resource. You have to use a Geolocation routing policy instead.