AWS Paper-1

Question 1:

A tech company has a CRM application hosted on an Auto Scaling group of On-Demand EC2 instances. The application is extensively used during office hours from 9 in the morning till 5 in the afternoon. Their users are complaining that the performance of the application is slow during the start of the day but then works normally after a couple of hours.

Which of the following can be done to ensure that the application works properly at the beginning of the day?

A. Configure a Dynamic scaling policy for the Auto Scaling group to launch new instances based on the CPU utilization.

B. Configure a Dynamic scaling policy for the Auto Scaling group to launch new instances based on the Memory utilization.

C. Configure a Scheduled scaling policy for the Auto Scaling group to launch new instances before the start of the day. (Correct)

D. Set up an Application Load Balancer (ALB) to your architecture to ensure that the traffic is properly distributed on the instances.

Explanation

Scaling based on a schedule allows you to scale your application in response to predictable load changes. For example, every week the traffic to your web application starts to increase on Wednesday, remains high on Thursday, and starts to decrease on Friday. You can plan your scaling activities based on the predictable traffic patterns of your web application.

To configure your Auto Scaling group to scale based on a schedule, you create a scheduled action. The scheduled action tells Amazon EC2 Auto Scaling to perform a scaling action at specified times. To create a scheduled scaling action, you specify the start time when the scaling action should take effect, and the new minimum, maximum, and desired sizes for the scaling action. At the specified time, Amazon EC2 Auto Scaling updates the group with the values for minimum, maximum, and desired size specified by the scaling action. You can create scheduled actions for scaling one time only or for scaling on a recurring schedule.

Option 3 is the correct answer. You need to configure a Scheduled scaling policy. This will ensure that the instances are already scaled up and ready before the start of the day since this is when the application is used the most.

Options 1 and 2 are because although this is a valid solution, it is still better to configure a Scheduled scaling policy as you already know the exact peak hours of your application. By the time either the CPU or Memory hits a peak, the application already has performance issues, so you need to ensure the scaling is done beforehand using a Scheduled scaling policy.

Option 4 is . Although the Application load balancer can also balance the traffic, it cannot increase the instances based on demand.

Question 2:
You are deploying an Interactive Voice Response (IVR) telephony system in your cloud architecture that interacts with callers, gathers information, and routes calls to the appropriate recipients in your company. The system will be composed of an Auto Scaling group of EC2 instances, an Application Load Balancer, and an RDS instance in a Multi-AZ Deployments configuration. To protect the confidential data of your customers, you must ensure that your RDS database can only be accessed using the profile credentials specific to your EC2 instances via an authentication token.

As the Solutions Architect of the company, which of the following should you do to meet the above requirement?

A. Enable the IAM DB Authentication. (Correct)
B. Configure SSL in your application to encrypt the database connection to RDS. **()**
C. Create an IAM Role and assign it to your EC2 instances which will grant exclusive access to your RDS instance.
D. Use a combination of IAM and STS to restrict access to your RDS instance via a temporary token.

Explanation

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

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

IAM database authentication provides the following benefits:

- Network traffic to and from the database is encrypted using Secure Sockets Layer (SSL).
- You can use IAM to centrally manage access to your database resources, instead of managing access individually on each DB instance.

- For applications running on Amazon EC2, you can use profile credentials specific to your EC2 instance to access your database instead of a password, for greater security

Hence, Option 1 is the correct answer based on the above reference.

Option 2 is because an SSL connection is not using an authentication token from IAM. Although configuring SSL to your application can improve the security of your data in flight, it is still not a suitable option to use in this scenario.

Option 3 is because although you can create and assign an IAM Role to your EC2 instances, you still need to configure your RDS to use IAM DB Authentication.

Option 4 is because you have to use IAM DB Authentication for this scenario, and not a combination of an IAM and STS. Although STS is used to send temporary tokens for authentication, this is not a compatible use case for RDS.

Question 3:
You founded a tech start-up that provides online training and software development courses to various students across the globe. Your team has developed an online portal in AWS where the students can log into and access the courses they are subscribed to.

Since you are in the early phases of the startup and the funding is still hard to come by, which service can help you manage the budgets for all your AWS resources?

A. Cost Explorer

B. Cost Allocation Tags

C. **AWS Budgets(Correct)**

D. Payment History

Explanation

AWS Budgets gives you the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount.

Budgets can be tracked at the monthly, quarterly, or yearly level, and you can customize the start and end dates. You can further refine your budget to track costs associated with multiple dimensions, such as AWS service, linked account, tag, and others. Budget alerts can be sent via email and/or Amazon Simple Notification Service (SNS) topic.

You can also use AWS Budgets to set a custom reservation utilization target and receive alerts when your utilization drops below the threshold you define. RI utilization alerts support Amazon EC2, Amazon RDS, Amazon Redshift, and Amazon ElastiCache reservations.

Budgets can be created and tracked from the AWS Budgets dashboard or via the Budgets API.

Option 1 is because the Cost Explorer only helps you visualize and manage your AWS costs and usages over time. It offers a set of reports you can view data with for up to the last 13 months, forecast how much you're likely to spend for the next three months, and get recommendations for what Reserved Instances to purchase. You use Cost Explorer to identify areas that need further inquiry and see trends to understand your costs.

Option 2 is because Cost Allocation Tags only eases the organization of your resource costs on your cost allocation report, to make it easier for you to categorize and track your AWS costs.

Option 4 is because the payment history option only provides a location where you can view the monthly invoices you receive from AWS. If your account isn't past due, the Payment History page shows only previous invoices and payment status.

Question 4:
You are trying to establish an SSH connection to a newly created Amazon EC2 instance using the PuTTY tool. However, you are getting the following error message:

What steps should you take to fix this issue?

A. Verify if your private key (.pem) file has been correctly converted to the format recognized by PuTTY (.ppk).(Correct)
B. Verify that your IAM user policy has permission to launch Amazon EC2 instances.
C. Verify that you are connecting with the appropriate user name for your AMI such as ec2-user for Linux AMI, centos for Centos AMI or admin for Debian AMI(Correct)
D. Verify that the Amazon EC2 Instance was launched with the proper IAM role.
E. Verify that you have waited at least 1 hour after the EC2 instance was created before connecting via SSH

Explanation

If you use PuTTY to connect to your instance via SSH and get either of the following errors, Error: Server refused our key or Error: No supported authentication methods available, verify that you are connecting with the appropriate user name for your AMI. Enter the user name in the **User name** box in the **PuTTY Configuration** window.

The appropriate user names are as follows:

- -For an Amazon Linux AMI, the user name is ec2-user.
- -For a RHEL AMI, the user name is ec2-user or root.

- -For an Ubuntu AMI, the user name is ubuntu or root.
- -For a Centos AMI, the user name is centos.
- -For a Debian AMI, the user name is admin or root.
- -For a Fedora AMI, the user name is ec2-user.
- -For a SUSE AMI, the user name is ec2-user or root.
- -Otherwise, if ec2-user and root don't work, check with the AMI provider.

You should also verify that your private key (.pem) file has been correctly converted to the format recognized by PuTTY (.ppk).

Options 2 and 4 are because both an IAM user and IAM role policy have nothing to do with this issue.

Option 5 is because you don't need to wait an hour in order to connect to a new EC2 instance as you can immediately connect to it once it is created.

Question 5:
A financial application that calculates accruals, interests, and other data is hosted on a fleet of Spot EC2 instances that are configured with Auto Scaling. The application is used by an external reporting application that provides the total calculation for each user account and transaction. You used CloudWatch to automatically monitor the EC2 instance without manually checking the server for high CPU Utilization or crashes.

What is the time period of data that Amazon CloudWatch receives and aggregates from EC2 by default?

A. One second
B. Five seconds
C. One minute
D. Five minutes (Correct)

Explanation

By default, your instance is enabled for basic monitoring. You can optionally enable detailed monitoring. After you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period for the instance. The following table describes basic and detailed monitoring for instances.

1. **Basic** - Data is available automatically in 5-minute periods at no charge.
2. **Detailed** - Data is available in 1-minute periods for an additional cost. To get this level of data, you must specifically enable it for the instance. For the instances

where you've enabled detailed monitoring, you can also get aggregated data across groups of similar instances.

Options 1 and 2 are because although you can publish Custom Metrics down to 1-second or 2-second resolution to give you more immediate visibility and greater granularity into the state and performance of your custom applications, these are not the default values in CloudWatch.

Option 3 is because the 1-minute data period is only available for detailed monitoring and it is not enabled by default.

Question 6:
You are a Solutions Architect of a bank, designing various CloudFormation templates for a new online trading platform that your department will build.

How much does it cost to use CloudFormation templates?

- **A. There is no additional charge for AWS CloudFormation. You only pay for the AWS resources that are created. (Correct)**
- B. The cost is based on the file size of the template.
- C. It is charged per hour.
- D. The cost is based on the size of the template.

Explanation

There is no additional charge for AWS CloudFormation. You only pay for the AWS resources that are created (e.g. Amazon EC2 instances, Elastic Load Balancing load balancers, etc.)

Question 7:
You are working as a Solutions Architect for a technology company which is in the process of migrating their applications to AWS. One of their systems requires a database that can scale globally and can handle frequent schema changes. It should also provide low-latency response to high-traffic queries.

Which is the most suitable database solution to use to achieve this requirement?

- A. An Amazon RDS instance in Multi-AZ Deployments configuration
- **B. Amazon DynamoDB (Correct)**
- C. An Amazon Aurora database with Read Replicas ()
- D. Redshift

Explanation

Before we proceed in answering this question, we must first be clear with the actual definition of a "**schema**". Basically, the english definition of a schema is: *a representation of a plan or theory in the form of an outline or model*.

Just think of a schema as the "structure" or a "model" of your data in your database. Since the scenario requires that the schema, or the structure of your data, changes frequently, then you have to pick a database which provides a non-rigid and flexible way of adding or removing new types of data. This is a classic example of choosing between a relational database and non-relational (NoSQL) database.

A relational database is known for having a rigid schema, with a lot of constraints and limits as to which (and what type of) data can be inserted or not. It is primarily used for scenarios where you have to support complex queries which fetch data across a number of tables. It is best for scenarios where you have complex table relationships but for use cases where you need to have a flexible schema, this is not a suitable database to use.

For NoSQL, it is not as rigid as a relational database because you can easily add or remove rows or elements in your table/collection entry. It also has a more flexible schema because it can store complex hierarchical data within a single item which, unlike a relational database, does not entail changing multiple related tables. Hence, the best answer to be used here is a NoSQL database, like DynamoDB. When your business requires a low-latency response to high-traffic queries, taking advantage of a NoSQL system generally makes technical and economic sense.

Amazon DynamoDB helps solve the problems that limit the relational system scalability by avoiding them. In DynamoDB, you design your schema specifically to make the most common and important queries as fast and as inexpensive as possible. Your data structures are tailored to the specific requirements of your business use cases.

Remember that a relational database system **does not scale** well for the following reasons:

- -It normalizes data and stores it on multiple tables that require multiple queries to write to disk.
- -It generally incurs the performance costs of an ACID-compliant transaction system.
- -It uses expensive joins to reassemble required views of query results.

For DynamoDB, it scales well due to these reasons:

- -Its **schema flexibility** lets DynamoDB store complex hierarchical data within a single item. DynamoDB is not a totally *schemaless* database since the very definition of a schema is just the model or structure of your data.
- -Composite key design lets it store related items close together on the same table.

Options 1 and 3 are because both of them are a type of relational database.

Option 4 is because Redshift is primarily used for OLAP systems.

Question 8:
You have one security group associated with 10 On-Demand EC2 instances. You then modified the security group to allow all inbound SSH traffic and then right after that, you created two new EC2 instances in the same security group.

When will the changes be applied to the EC2 instances?

A. **Immediately to all 12 instances in the security group. (Correct)**
B. Immediately to the new instances only.
C. Immediately to the new instances, but not for the old ones which must be restarted before the changes take effect.
D. The changes will apply to all 12 instances after an hour when the propagation is complete.

Explanation

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

Option 1 is correct. When you add or remove rules, those changes are automatically applied to all instances to which you've assigned the security group. Since the first 10 instances are already assigned to the security group, you can SSH into them immediately after the change. After adding the two new instances to the security group, you should be able to SSH into them as well since the change was made beforehand.

Options 2 and 3 are because the changes will be applied to all EC2 instances and not just to the new or old set of instances.

Option 4 is because you don't have to wait for an hour for the changes to be applied to your security group since the changes will be immediately reflected.

Question 9:
The company that you are working for has a highly available architecture consisting of an elastic load balancer and several EC2 instances configured with auto-scaling in three Availability Zones. You want to monitor your EC2 instances based on a particular metric, which is not readily available in CloudWatch.

Which of the following is a custom metric in CloudWatch which you have to manually set up?

A. **Memory Utilization of an EC2 instance (Correct)**
B. CPU Utilization of an EC2 instance
C. Disk Reads activity of an EC2 instance
D. Network packets out of an EC2 instance

Explanation

CloudWatch has available Amazon EC2 Metrics for you to use for monitoring. CPU Utilization identifies the processing power required to run an application upon a selected instance. Network Utilization identifies the volume of incoming and outgoing network traffic to a single instance. Disk Reads metric is used to determine the volume of the data the application reads from the hard disk of the instance. This can be used to determine the speed of the application. However, there are certain metrics that are not readily available in CloudWatch such as memory utilization, disk space utilization, and many others which can be collected by setting up a custom metric.

You need to prepare a custom metric using CloudWatch Monitoring Scripts which is written in Perl. You can also install CloudWatch Agent to collect more system-level metrics from Amazon EC2 instances. Here's the list of custom metrics that you can set up:

- Memory utilization
- Disk swap utilization
- Disk space utilization
- Page file utilization
- Log collection

Options 2, 3, and 4 are because these metrics are readily available in CloudWatch by default.

Question 10:
You are leading a software development team which uses serverless computing with AWS Lambda to build and run applications without having to set up or manage servers. You have a Lambda function that connects to a MongoDB Atlas, which is a popular Database as a Service (DBaaS) platform and also uses a third party API to fetch certain data for your application. You instructed one of your junior developers to create the environment variables for the MongoDB database hostname, username, and password as well as the API credentials that will be used by the Lambda function for DEV, SIT, UAT and PROD environments.

Considering that the Lambda function is storing sensitive database and API credentials, how can you secure these information to prevent other developers in your team, or anyone, from seeing these credentials in plain text? Select the best option that provides the maximum security.

A. There is no need to do anything because, by default, AWS Lambda already encrypts the environment variables using the AWS Key Management Service.()

B. Enable SSL encryption that leverages on AWS CloudHSM to store and encrypt the sensitive information.
C. AWS Lambda does not provide encryption for the environment variables. Deploy your code to an EC2 instance instead.
D. Create a new KMS key and use it to enable encryption helpers that leverage on AWS Key Management Service to store and encrypt the sensitive information. (Correct)

Explanation

When you create or update Lambda functions that use environment variables, AWS Lambda encrypts them using the AWS Key Management Service. When your Lambda function is invoked, those values are decrypted and made available to the Lambda code.

The first time you create or update Lambda functions that use environment variables in a region, a default service key is created for you automatically within AWS KMS. This key is used to encrypt environment variables. However, if you wish to use encryption helpers and use KMS to encrypt environment variables after your Lambda function is created, you must create your own AWS KMS key and choose it instead of the default key. The default key will give errors when chosen. Creating your own key gives you more flexibility, including the ability to create, rotate, disable, and define access controls, and to audit the encryption keys used to protect your data.

Option 1 is since Lambda does not encrypt environment variables by default during the deployment process. When you deploy your Lambda function, all the environment variables you've specified are encrypted by default after, but not during, the deployment process.

Option 2 is also since enabling SSL would encrypt data only when in-transit. Your other teams would still be able to view the plaintext at-rest. Use AWS KMS instead.

Option 3 is since, as mentioned, Lambda does provide encryption functionality of environment variables.

Question 11:
In your AWS VPC, you need to add a new subnet that will allow you to host a total of 20 EC2 instances.

Which of the following IPv4 CIDR block can you use for this scenario?

A. 172.0.0.0/27(Correct)
B. 172.0.0.0/28()
C. 172.0.0.0/29
D. 172.0.0.0/30

Explanation

To calculate the total number of IP addresses of a given CIDR Block, you simply need to follow the 2 easy steps below. Let's say you have a CIDR block **/27**:

1. Subtract **32** with the mask number :

(32 - 27) = **5**

2. Raise the number **2** to the power of the answer in Step #1 :

2^ **5** = (2 * 2 * 2 * 2 * 2)

= **32**

The answer to Step #2 is the total number of IP addresses available in the given CIDR netmask. Don't forget that in AWS, the first 4 IP addresses and the last IP address in each subnet CIDR block are not available for you to use, and cannot be assigned to an instance. In addition, you can always associate a netmask of /27 which also has the same number of usable IP addresses (27) to help you with your exam.

Option 1 is the correct answer because the CIDR block of 172.0.0.0/27, with a netmask of /27, has an equivalent of 27 *usable* IP addresses. Take note that a netmask of /27 originally provides you with 32 IP addresses but in AWS, there are 5 IP addresses that are reserved which you cannot use. The first 4 IP addresses and the last IP address in each subnet CIDR block are not available in your VPC which means that you have to **always** subtract 5 IP addresses, hence 32 - 5 = 27.

Option 2 is as a netmask of /28 only supports 16 IP Addresses.

Options 3 and 4 are as the only allowed block size is between a /28 netmask and /16 netmask.

To add a CIDR block to your VPC, the following rules apply:

- -The allowed block size is between a /28 netmask and /16 netmask.
- -The CIDR block must not overlap with any existing CIDR block that's associated with the VPC.
- -You cannot increase or decrease the size of an existing CIDR block.
- -You have a limit on the number of CIDR blocks you can associate with a VPC and the number of routes you can add to a route table. You cannot associate a CIDR block if this results in you exceeding your limits.
- -The CIDR block must not be the same or larger than the CIDR range of a route in any of the VPC route tables. For example, if you have a route with a destination of 10.0.0.0/24 to a virtual private gateway, you cannot associate a CIDR block of the same range or larger. However, you can associate a CIDR block of 10.0.0.0/25 or smaller.

- -The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use, and cannot be assigned to an instance.

Question 12:
A traffic monitoring and reporting application uses Kinesis to accept real-time data. In order to process and store the data, they used Amazon Kinesis Data Firehose to load the streaming data to various AWS resources.

Which of the following services can you load streaming data into?

A. Amazon S3 Select
B. Amazon Redshift Spectrum ()
C. Amazon Elasticsearch Service (Correct)
D. Amazon Athena

Explanation

Amazon Kinesis Data Firehose is the easiest way to load streaming data into data stores and analytics tools. It can capture, transform, and load streaming data into Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk, enabling near real-time analytics with existing business intelligence tools and dashboards you're already using today.

It is a fully managed service that automatically scales to match the throughput of your data and requires no ongoing administration. It can also batch, compress, and encrypt the data before loading it, minimizing the amount of storage used at the destination and increasing security.

Options 1 and 2 are because Amazon S3 ***Select*** is just a feature of Amazon S3. Likewise, Redshift ***Spectrum*** is also just a feature of Amazon Redshift. Although Amazon Kinesis Data Firehose can load streaming data to both Amazon S3 and Amazon Redshift, it does not directly load the data to S3 Select and Redshift Spectrum.

S3 Select is an Amazon S3 feature that makes it easy to retrieve specific data from the contents of an object using simple SQL expressions without having to retrieve the entire object. Amazon Redshift Spectrum is a feature of Amazon Redshift that enables you to run queries against exabytes of unstructured data in Amazon S3 with no loading or ETL required.

Option 4 is because Amazon Kinesis Data Firehose cannot load streaming data to Athena.

Question 13:
You are managing a suite of applications in your on-premises network which are using trusted IP addresses that your partners and customers have whitelisted in their firewalls. There is a requirement to migrate these applications to AWS

without requiring your partners and customers to change their IP address whitelists.

Which of the following is the most suitable solution to properly migrate your applications?

A. Set up a list of Elastic IP addresses to map the whitelisted IP address range in your on-premises network.()
B. Set up an IP match condition using a CloudFront web distribution and AWS WAF to whitelist a specific IP address range in your VPC.
C. Create a Route Origin Authorization (ROA) then once done, provision and advertise your whitelisted IP address range to your AWS account.(Correct)
D. Submit an AWS Request Form to migrate the IP address range that you own to your AWS Account.

Explanation

You can bring part or all of your public IPv4 address range from your on-premises network to your AWS account. You continue to own the address range, but AWS advertises it on the Internet. After you bring the address range to AWS, it appears in your account as an address pool. You can create an Elastic IP address from your address pool and use it with your AWS resources, such as EC2 instances, NAT gateways, and Network Load Balancers. This is also called "Bring Your Own IP Addresses (BYOIP)".

To ensure that only you can bring your address range to your AWS account, you must authorize Amazon to advertise the address range and provide proof that you own the address range.

A **Route Origin Authorization (ROA)** is a document that you can create through your Regional internet registry (RIR), such as the American Registry for Internet Numbers (ARIN) or Réseaux IP Européens Network Coordination Centre (RIPE). It contains the address range, the ASNs that are allowed to advertise the address range, and an expiration date. Hence, Option 3 is the correct answer.

The ROA authorizes Amazon to advertise an address range under a specific AS number. However, it does not authorize your AWS account to bring the address range to AWS. To authorize your AWS account to bring an address range to AWS, you must publish a self-signed X509 certificate in the RDAP remarks for the address range. The certificate contains a public key, which AWS uses to verify the authorization-context signature that you provide. You should keep your private key secure and use it to sign the authorization-context message.

Option 1 is because you cannot map the IP address of your on-premises network, which you are migrating to AWS, to an EIP address of your VPC. To satisfy the requirement, you must authorize Amazon to advertise the address range that you own.

Option 2 is because the IP match condition in CloudFront is primarily used in allowing or blocking the incoming web requests based on the IP addresses that the requests

originate from. This is the opposite of what is being asked in the scenario, where you have to migrate your suite of applications from your on-premises network and advertise the address range that you own in your VPC.

Option 4 is because you don't need to submit an AWS request in order to do this. You can simply create a Route Origin Authorization (ROA) then once done, provision and advertise your whitelisted IP address range to your AWS account.

Question 14:
There was an incident in your production environment where the user data stored in the S3 bucket has been accidentally deleted by one of the Junior DevOps Engineers. The issue was escalated to your manager and after a few days, you were instructed to improve the security and protection of your AWS resources.

What combination of the following options will protect the S3 objects in your bucket from both accidental deletion and overwriting? (Choose 2)

- **A. Enable Versioning (Correct)**
- B. Provide access to S3 data strictly through pre-signed URL only
- C. Disallow S3 Delete using an IAM bucket policy
- D. Enable Amazon S3 Intelligent-Tiering
- **E. Enable Multi-Factor Authentication Delete (Correct)**

Explanation

By using Versioning and enabling MFA (Multi-Factor Authentication) Delete, you can secure and recover your S3 objects from accidental deletion or overwrite.

Versioning is a means of keeping multiple variants of an object in the same bucket. Versioning-enabled buckets enable you to recover objects from accidental deletion or overwrite. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures.

You can also optionally add another layer of security by configuring a bucket to enable MFA (Multi-Factor Authentication) Delete, which requires additional authentication for either of the following operations:

- Change the versioning state of your bucket

- Permanently delete an object version

MFA Delete requires two forms of authentication together:

- Your security credentials

- The concatenation of a valid serial number, a space, and the six-digit code displayed on an approved authentication device

Option 2 is since a pre-signed URL gives access to the object identified in the URL. Pre-signed URLs are useful when customers perform an object upload to your S3 bucket, but does not help in preventing accidental deletes.

Option 3 is since you still want users to be able to delete objects in the bucket, and you just want to prevent accidental deletions. Disallowing S3 Delete using an IAM bucket policy will restrict all delete operations to your bucket.

Option 4 is since S3 intelligent tiering does not help in this situation.

Question 15:
You have a web application deployed in AWS which is currently running in the eu-central-1 region. You have an Auto Scaling group of On-Demand EC2 instances which are using pre-built AMIs. Your manager instructed you to implement disaster recovery for your system so in the event that the application goes down in the eu-central-1 region, a new instance can be started in the us-west-2 region.

As part of your disaster recovery plan, which of the following should you take into consideration?

A. In the AMI dashboard, add the us-west-2 region to the Network Access Control List which contains the regions that are allowed to use the AMI.
B. Copy the AMI from the eu-central-1 region to the us-west-2 region. Afterwards, create a new Auto Scaling group in the us-west-2 region to use this new AMI ID.(Correct)
C. Share the AMI to the us-west-2 region.
D. None. AMIs can be used in any region hence, there is no problem using it in the us-west-2 region.

Explanation

In this scenario, the EC2 instances you are currently using depends on a pre-built AMI. This AMI is not accessible to another region hence, you have to copy it to the us-west-2 region to properly establish your disaster recovery instance.

You can copy an Amazon Machine Image (AMI) within or across an AWS region using the AWS Management Console, the AWS command line tools or SDKs, or the Amazon EC2 API, all of which support the CopyImage action. You can copy both Amazon EBS-backed AMIs and instance store-backed AMIs. You can copy encrypted AMIs and AMIs with encrypted snapshots.

Options 1 and 3 are because the AMI does not have a Network Access Control nor a Share functionality.

Option 4 is as you can use a unique or pre-built AMI to a specific region only.

Question 16:
A popular mobile game uses CloudFront, Lambda, and DynamoDB for its backend services. The player data is persisted on a DynamoDB table and the static assets are distributed by CloudFront. However, there are a lot of complaints that saving and retrieving player information is taking a lot of time.

To improve the game's performance, which AWS service can you use to reduce DynamoDB response times from milliseconds to microseconds?

A. Amazon Elasticsearch
B. AWS Device Farm
C. DynamoDB Auto Scaling ()
D. Amazon DynamoDB Accelerator (DAX)(Correct)

Explanation

Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache that can reduce Amazon DynamoDB response times from milliseconds to microseconds, even at millions of requests per second.

Option 1 is because the Amazon Elasticsearch service is a fully managed service that makes it easy for you to deploy, secure, operate, and scale your Elasticsearch engine to search, analyze, and visualize data in real-time. Although you may integrate Elasticsearch with DynamoDB, it will not reduce the DynamoDB response time from milliseconds to microseconds, even at millions of requests per second, whereas DynamoDB DAX can.

Option 2 is because AWS Device Farm is an app testing service that lets you test and interact with your Android, iOS, and web apps on many devices at once, or reproduce issues on a device in real time.

Option 3 is because DynamoDB Auto Scaling is primarily used to automate capacity management for your tables and global secondary indexes.

Question 17:
You have launched a new enterprise application with a web server and a database. You are using a large EC2 Instance with one 500 GB EBS volume to host a relational database. Upon checking the performance, it shows that write throughput to the database needs to be improved.

Which of the following is the most suitable configuration to help you achieve this requirement?

A. Set up a standard RAID 0 configuration with two EBS Volumes (Correct)

B. Re-launch the instance with a Paravirtual (PV) AMI and enable Enhanced Networking ()
C. Use a standard RAID 1 configuration with two EBS Volumes
D. Set up the EC2 instance in a placement group
E. Increase the size of the EC2 Instance (Correct)

Explanation

The goal here is to increase the write performance of the database hosted in an EC2 instance. You can achieve this by either setting up a standard RAID 0 configuration or simply by increasing the size of the EC2 instance.

Some EC2 instance types can drive more I/O throughput than what you can provision for a single EBS volume. You can join multiple gp2, io1, st1, or sc1 volumes together in a RAID 0 configuration to use the available bandwidth for these instances.

With Amazon EBS, you can use any of the standard RAID configurations that you can use with a traditional bare metal server, as long as that particular RAID configuration is supported by the operating system for your instance. This is because all RAID is accomplished at the software level. For greater I/O performance than you can achieve with a single volume, RAID 0 can stripe multiple volumes together; for on-instance redundancy, RAID 1 can mirror two volumes together.

Take note that HVM AMIs are required to take advantage of enhanced networking and GPU processing. In order to pass through instructions to specialized network and GPU devices, the OS needs to be able to have access to the native hardware platform which the HVM virtualization provides.

Option 2 is because although the Enhanced Networking feature can provide higher I/O performance and lower CPU utilization to your EC2 instance, you have to use an HVM AMI instead of PV AMI.

Option 3 is because the main use case for RAID 1 is to provide mirroring, redundancy, and fault-tolerance. RAID 0 is a more suitable option for providing faster read and write operations, compared with RAID 1.

Option 4 is because the placement groups feature is primarily used for inter-instance communication.

Question 18:
In a government agency that you are working for, you have been assigned to put confidential tax documents on AWS cloud. However, there is a concern from a security perspective on what can be put on AWS.

What are the features in AWS that can ensure data security for your confidential documents?

A. EBS On-Premises Data Encryption

B. S3 Server-Side Encryption (Correct)
C. S3 Client-Side Encryption (Correct)
D. Public Data Set Volume Encryption
E. S3 On-Premises Data Encryption

Explanation

You can secure the privacy of your data in AWS, both at rest and in-transit, through encryption. If your data is stored in EBS Volumes, you can enable EBS Encryption and if it is stored on Amazon S3, you can enable client-side and server-side encryption.

Option 4 is as public data sets are designed to be publicly accessible.

Options 1 and 5 are as there is no such thing as On-Premises Data Encryption for S3 and EBS as these services are in the AWS cloud and not on your on-premises network.

Question 19:
You are working for a large pharmaceutical company that has resources hosted on both their on-premises network and in AWS cloud. They want all of their Software Architects to access resources on both environments using their on-premises credentials, which is stored in Active Directory.

In this scenario, which of the following can be used to fulfill this requirement?

A. Use Web Identity Federation
B. Use SAML Federation (Correct)
C. Use IAM users
D. Use AWS VPC

Explanation

Since the company is using Microsoft Active Directory which implements Security Assertion Markup Language (SAML), you can set up a SAML-Based Federation for API Access to your AWS cloud. In this way, you can easily connect to AWS using the login credentials of your on-premises network.

AWS supports identity federation with SAML 2.0, an open standard that many identity providers (IdPs) use. This feature enables federated single sign-on (SSO), so users can log into the AWS Management Console or call the AWS APIs without you having to create an IAM user for everyone in your organization. By using SAML, you can simplify the process of configuring federation with AWS, because you can use the IdP's service instead of writing custom identity proxy code.

Option 1 is because web identity federation is primarily used to let users sign in via a well-known external identity provider (IdP), such as Login with Amazon, Facebook, Google. It does not utilize Active Directory.

Option 3 is because the situation requires you to use the existing credentials stored in their Active Directory, and not user accounts that will be generated by IAM.

Option 4 is because the AWS VPC lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. This has nothing to do with user authentication or Active Directory.

Question 20:
You are a Solutions Architect working for a major telecommunications company in Europe. You deployed an On-Demand EC2 instance that is transferring large amounts of data to an Amazon S3 bucket in the same region. Your manager is worried about infrastructure cost considering the vast amounts of data being transferred to the bucket.

What will you say to justify this architecture?

A. You are only using an On-Demand EC2 instance which is exactly the same price as Spot EC2 instance, launched by a persistent Spot request.
B. Transferring data from an EC2 instance to an S3 bucket in the same region has no cost at all. (Correct)
C. Transferring data from an EC2 instance to an S3 bucket in the same region has a 50% discount based on the AWS Pricing.
D. You are only using an On-Demand EC2 instance so the cost will be lower than a Spot instance.

Explanation

Transferring data from an EC2 instance to Amazon S3, Amazon Glacier, Amazon DynamoDB, Amazon SES, Amazon SQS, or Amazon SimpleDB in the same AWS Region has no cost at all. Refer to the Amazon EC2 Pricing on the link below for reference.

Options 1 and 4 are since an On-Demand instance costs more than a Spot instance.

Option 3 is as there is no such thing as 50% discount when transferring data from an EC2 instance to an S3 bucket in the same region.

Question 21:
A telecommunications company is planning to give AWS Console access to developers. Company policy mandates the use of identity federation and role-based access control. Currently, the roles are already assigned using groups in the corporate Active Directory.

In this scenario, what combination of the following services can provide developers access to the AWS console? (Choose 2)

A. AWS Directory Service AD Connector (Correct)
B. AWS Directory Service Simple AD()

C. IAM Groups
D. IAM Roles (Correct)
E. Lambda

Explanation

Considering that the company is using a corporate Active Directory, it is best to use AWS Directory Service AD Connector for easier integration. In addition, since the roles are already assigned using groups in the corporate Active Directory, it would be better to also use IAM Roles. Take note that you can assign an IAM Role to the users or groups from your Active Directory once it is integrated with your VPC via the AWS Directory Service AD Connector.

AWS Directory Service provides multiple ways to use Amazon Cloud Directory and Microsoft Active Directory (AD) with other AWS services. Directories store information about users, groups, and devices, and administrators use them to manage access to information and resources. AWS Directory Service provides multiple directory choices for customers who want to use existing Microsoft AD or Lightweight Directory Access Protocol (LDAP)–aware applications in the cloud. It also offers those same choices to developers who need a directory to manage users, groups, devices, and access.

Question 22:
You are tasked to host a web application in a new VPC with private and public subnets. In order to do this, you will need to deploy a new MySQL database server and a fleet of EC2 instances to host the application. In which subnet should you launch the new database server into?

A. The public subnet
B. The private subnet(Correct)
C. Either public or private subnet
D. Ideally be launched outside the Amazon VPC

Explanation

In an ideal and secure VPC architecture, you launch the web servers or elastic load balancers in the public subnet and the database servers in the private subnet.

Option 1 is because if you launch your database server in the public subnet, it will be publicly accessible all over the Internet which has a higher security risk.

Option 2 is correct because it is more secure to launch your database in the private subnet to prevent other external and unauthorized users to access or attack your system.

Option 3 is since only the private subnet is the correct answer if you want to secure your database from external traffic.

Option 4 is as there is no need to launch it outside the VPC. Having it run in a private subnet should address the security and networking concerns of your database.

Question 23:
An application that records weather data every minute is deployed in a fleet of Spot EC2 instances and uses a MySQL RDS database instance. Currently, there is only one RDS instance running in one Availability Zone. You plan to improve the database to ensure high availability and scalability by synchronous data replication to another RDS instance.

Which of the following performs synchronous data replication in RDS?

- **A. RDS DB instance running as a Multi-AZ deployment(Correct)**
- B. RDS Read Replica in Oracle Database
- C. DynamoDB Read Replica
- D. CloudFront running as a Multi-AZ deployment

Explanation

When you create or modify your DB instance to run as a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous **standby** replica in a different Availability Zone. Updates to your DB Instance are synchronously replicated across Availability Zones to the standby in order to keep both in sync and protect your latest database updates against DB instance failure.

Option 2 is as a Read Replica provides an asynchronous replication instead of synchronous. In addition, a Read Replica is only available in Aurora, MySQL, MariaDB, and PostgreSQL database engines.

Options 3 and 4 are wrong answers as both DynamoDB and CloudFront do not have a Read Replica feature.

Question 24:
You are a newly-hired Solutions Architect in a leading utilities provider, which is in the process of migrating their applications to AWS. You created an EBS-Backed EC2 instance with ephemeral0 and ephemeral1 instance store volumes attached to host a web application that fetches and stores data from a web API service.

If this instance is stopped, what will happen to the data on the ephemeral store volumes?

- A. Data is automatically saved in an EBS volume.
- B. Data is unavailable until the instance is restarted.
- **C. Data will be deleted. (Correct)**
- D. Data is automatically saved as an EBS snapshot.

Explanation

The word ***ephemeral*** means *"short-lived"* or *"temporary"* in the English dictionary. Hence, when you see this word in AWS, always consider this as just a temporary memory or a short-lived storage.

The virtual devices for instance store volumes are named as ephemeral[0-23]. Instance types that support one instance store volume have ephemeral0. Instance types that support two instance store volumes have ephemeral0 and ephemeral1, and so on until ephemeral23.

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

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

Hence, Option 3 is the correct answer.

Option 1 is since instance store volumes and EBS volumes are two different storage types. An Amazon EBS volume is a durable, block-level storage device that you can attach to a single EC2 instance. An instance store provides temporary block-level storage and is located on disks that are physically attached to the host computer. No automatic backup will be performed.

Option 2 is because once you stop an instance, the data in the ephemeral instance store volumes will be gone.

Option 4 is because like Option 2, instance store volumes and EBS volumes are two different storage devices. There is no automated snapshot that will be created.

Question 25:

An online cryptocurrency exchange platform is hosted in AWS which uses ECS Cluster and RDS in Multi-AZ Deployments configuration. The application is heavily using the RDS instance to process complex read and write database operations. To maintain the reliability, availability, and performance of your systems, you have to closely monitor how the different processes or threads on a DB instance use the CPU, including the percentage of the CPU bandwidth and total memory consumed by each process.

Which of the following is the most suitable solution to properly monitor your database?

A. Use Amazon CloudWatch to monitor the CPU Utilization of your database.

B. Create a script that collects and publishes custom metrics to CloudWatch, which tracks the real-time CPU Utilization of the RDS instance, and then set up a custom CloudWatch dashboard to view the metrics.
C. Enable Enhanced Monitoring in RDS.(Correct)
D. Check the CPU% and MEM% metrics which are readily available in the Amazon RDS console that shows the percentage of the CPU bandwidth and total memory consumed by each database process of your RDS instance.

Explanation

Amazon RDS provides metrics in real time for the operating system (OS) that your DB instance runs on. You can view the metrics for your DB instance using the console, or consume the Enhanced Monitoring JSON output from CloudWatch Logs in a monitoring system of your choice. By default, Enhanced Monitoring metrics are stored in the CloudWatch Logs for 30 days. To modify the amount of time the metrics are stored in the CloudWatch Logs, change the retention for the RDSOSMetrics log group in the CloudWatch console.

Take note that there are certain differences between CloudWatch and Enhanced Monitoring Metrics. CloudWatch gathers metrics about CPU utilization from the hypervisor for a DB instance, and Enhanced Monitoring gathers its metrics from an agent on the instance. As a result, you might find differences between the measurements, because the hypervisor layer performs a small amount of work. Hence, Option 3 is the correct answer in this specific scenario.

The differences can be greater if your DB instances use smaller instance classes, because then there are likely more virtual machines (VMs) that are managed by the hypervisor layer on a single physical instance. Enhanced Monitoring metrics are useful when you want to see how different processes or threads on a DB instance use the CPU.

Option 1 is because although you can use Amazon CloudWatch to monitor the CPU Utilization of your database instance, it does not provide the percentage of the CPU bandwidth and total memory consumed by each database process in your RDS instance. Take note that CloudWatch gathers metrics about CPU utilization from the hypervisor for a DB instance while RDS Enhanced Monitoring gathers its metrics from an agent on the instance.

Option 2 is because although you can use Amazon CloudWatch Logs and CloudWatch dashboard to monitor the CPU Utilization of the database instance, using CloudWatch alone is still not enough to get the specific percentage of the CPU bandwidth and total memory consumed by each database processes. The data provided by CloudWatch is not as detailed as compared with the Enhanced Monitoring feature in RDS. Take note as well that you do not have direct access to the instances/servers of your RDS database instance, unlike with your EC2 instances where you can install a CloudWatch agent or a custom script to get CPU and memory utilization of your instance.

Option 4 is because the CPU% and MEM% metrics are not readily available in the Amazon RDS console, which is contrary to what is being stated in this option.

Question 26:
You are a Solutions Architect for a leading Enterprise Resource Planning (ERP) solutions provider and you are instructed to design and set up the architecture of your ERP application in AWS. Your manager instructed you to avoid using fully-managed AWS services and instead, only use specific services which allows you to access the underlying operating system for the resource. This is to allow the company to have a much better control of the underlying resources that their systems are using in the AWS cloud.

Which of the following services should you choose to satisfy this requirement? (Choose 2)

A. Amazon Athena
B. Amazon EMR(Correct)
C. Amazon EC2(Correct)
D. DynamoDB
E. Amazon Neptune

Explanation

Amazon EC2 provides you access to the operating system of the instance that you created.

Amazon EMR provides you a managed Hadoop framework that makes it easy, fast, and cost-effective to process vast amounts of data across dynamically scalable Amazon EC2 instances. You can access the operating system of these EC2 instances that were created by Amazon EMR.

Options 1, 4 and 5 are as these are managed services, which means that AWS manages the underlying operating system and other server configurations that these databases use.

Question 27:
In the VPC that you are managing, it has one EC2 instance that has its data stored in an instance store. The instance was shut down by a 2nd level support staff over the weekend to save costs. When you arrived in the office the next Monday, you noticed that all data are lost and are no longer available on the EC2 instance.

What might be the cause of this?

A. The EC2 instance was using an instance store hence, data will be erased when the instance is terminated.(Correct)
B. The EC2 instance was using EBS-backed root volumes hence, the data will be erased when the instance is terminated.()

C. AWS automatically erased the data due to a virus found on the EC2 instance.
D. The EC2 instance has been hacked.

Explanation

Since you are using an EC2 instance with an Instance store, the data is ephemeral and it is expected to be erased once the instance is terminated. You may argue that the instance was only shut down but remember that the Operating system shutdown commands always terminate an instance store-backed instance. That is why the right answer is Option 1.

Amazon EC2 provides you with flexible, cost-effective, and easy-to-use data storage options for your instances. Each option has a unique combination of performance and durability. These storage options can be used independently or in combination to suit your requirements. These storage options include the following:

- -Amazon Elastic Block Store (EBS)
- -Amazon EC2 Instance Store
- -Amazon Elastic File System (Amazon EFS)
- -Amazon Simple Storage Service (Amazon S3)

If you used Amazon Elastic Block Store as the storage option of your instance, the data will exist independently of the life of your instance. This means that you configure the EBS volume to still exist even if you terminate your instance. If you are using an Instance Store as a storage option, the data is ephemeral and as the name implies, your data lasts for a very short time and would not exist once your EC2 instance is terminated.

Question 28:
You have a requirement to make sure that an On-Demand EC2 instance can only be accessed from this IP address (110.238.98.71) via an SSH connection. Which configuration below will satisfy this requirement?

A. Security Group Inbound Rule: Protocol – TCP. Port Range – 22, Source 110.238.98.71/32(Correct)
B. Security Group Inbound Rule: Protocol – UDP, Port Range – 22, Source 110.238.98.71/32
C. Security Group Inbound Rule: Protocol – TCP. Port Range – 22, Source 110.238.98.71/0
D. Security Group Inbound Rule: Protocol – UDP, Port Range – 22, Source 110.238.98.71/0

Explanation

The SSH protocol uses TCP and port 22. Hence, Options 2 and 4 are as they are using UDP. Options 1 and 3 have one major difference and that is their CIDR block

The requirement is to only allow the individual IP of the client and not the entire network. Therefore, the proper CIDR notation should be used. The **/32** denotes one IP address and the **/0** refers to the entire network. That is why Option 3 is as it allowed the entire network instead of a single IP.

Question 29:
There are many clients complaining that the online trading application of an investment bank is always down. Your manager instructed you to re-design the architecture of the application to prevent the unnecessary service interruptions. To ensure high availability, you set up the application to use an ELB to distribute the incoming requests across an auto-scaled group of EC2 instances in two single Availability Zones.

In this scenario, what happens when an EC2 instance behind an ELB fails a health check?

A. The EC2 instance gets terminated automatically by the ELB.
B. The EC2 instance gets quarantined by the ELB for root cause analysis.()
C. The EC2 instance is replaced automatically by the ELB.
D. The ELB stops sending traffic to the EC2 instance(Correct)

Explanation

In this scenario, the load balancer will route the incoming requests only to the healthy instances. When the load balancer determines that an instance is unhealthy, it stops routing requests to that instance. The load balancer resumes routing requests to the instance when it has been restored to a healthy state.

There are two ways of checking the status of your EC2 instances:

1. Via the Auto Scaling group

2. Via the ELB health checks

The default health checks for an Auto Scaling group are **EC2 status checks** only. If an instance fails these status checks, the Auto Scaling group considers the instance unhealthy and replaces. If you attached one or more load balancers or target groups to your Auto Scaling group, the group does not, by default, consider an instance unhealthy and replace it if it fails the load balancer health checks.

However, you can optionally configure the Auto Scaling group to use Elastic Load Balancing health checks. This ensures that the group can determine an instance's

health based on additional tests provided by the load balancer. The load balancer periodically sends pings, attempts connections, or sends requests to test the EC2 instances. These tests are called ***health checks.***

If you configure the Auto Scaling group to use Elastic Load Balancing health checks, it considers the instance unhealthy if it fails either the EC2 status checks or the load balancer health checks. If you attach multiple load balancers to an Auto Scaling group, all of them must report that the instance is healthy in order for it to consider the instance healthy. If one load balancer reports an instance as unhealthy, the Auto Scaling group replaces the instance, even if other load balancers report it as healthy.

Question 30:
A tech company that you are working for has undertaken a Total Cost Of Ownership (TCO) analysis evaluating the use of Amazon S3 versus acquiring more storage hardware. The result was that all 1200 employees would be granted access to use Amazon S3 for storage of their personal documents.

Which of the following will you need to consider so you can set up a solution that incorporates single sign-on feature from your corporate AD or LDAP directory and also restricts access for each individual user to a designated user folder in an S3 bucket?

A. Use 3rd party Single Sign-On solutions such as Atlassian Crowd, OKTA, OneLogin and many others.
B. Set up a Federation proxy or an Identity provider and use AWS Security Token Service to generate temporary tokens.(Correct)
C. Use a resource tag on each folder in the S3 bucket.
D. Configure an IAM role and an IAM Policy to access the bucket.(Correct)
E. Setup up a matching IAM user for each 1200 users in your corporate directory that needs access to a folder in the S3 bucket.

Explanation

The question refers to one of the common scenarios for temporary credentials in AWS. Temporary credentials are useful in scenarios that involve identity federation, delegation, cross-account access, and IAM roles. In this example, it is called **enterprise identity federation** considering that you also need to set up a single sign-on (SSO) capability.

The correct answers are:

- Setup a Federation proxy or an Identity provider

- Setup an AWS Security Token Service to generate temporary tokens (Option 2)

- Configure an IAM role (Option 4)

In an enterprise identity federation, you can authenticate users in your organization's network, and then provide those users access to AWS without creating new AWS identities for them and requiring them to sign in with a separate user name and password. This is known as the *single sign-on* (SSO) approach to temporary access. AWS STS supports open standards like Security Assertion Markup Language (SAML) 2.0, with which you can use Microsoft AD FS to leverage your Microsoft Active Directory. You can also use SAML 2.0 to manage your own solution for federating user identities.

Option 1 is since you don't have to use 3rd party solutions to provide the access. AWS already provides the necessary tools that you can use in this situation.

Option 3 is since placing resource tags on each folder won't help restrict access to a specific user.

Option 5 is since creating that many IAM users would be unnecessary. Also, you want the account to integrate with your AD or LDAP directory, hence, IAM Users does not fit these criteria.

Question 31:
You have a web application hosted in EC2 that consumes messages from an SQS queue and is integrated with SNS to send out an email to you once the process is complete. You received 5 orders but after a few hours, you saw more than 20 email notifications in your inbox.

Which of the following could be the possible culprit for this issue?

A. The web application is set for long polling so the messages are being sent twice.
B. The web application is not deleting the messages in the SQS queue after it has processed them.(Correct)
C. The web application is set to short polling so some messages are not being picked up()
D. The web application does not have permission to consume messages in the SQS queue**.**

Explanation

Always remember that the messages in the SQS queue will continue to exist even after the EC2 instance has processed it, until you delete that message. You have to ensure that you delete the message after processing to prevent the message from being received and processed again once the visibility timeout expires.

There are three main parts in a distributed messaging system:

1. The components of your distributed system (EC2 instances)

2. Your queue (distributed on Amazon SQS servers)

3. Messages in the queue.

You can set up a system which has several components that send messages to the queue and receive messages from the queue. The queue redundantly stores the messages across multiple Amazon SQS servers.

Refer to the third step of the SQS Message Lifecycle:

1. Component 1 sends Message A to a queue, and the message is distributed across the Amazon SQS servers redundantly.
2. When Component 2 is ready to process a message, it consumes messages from the queue, and Message A is returned. While Message A is being processed, it remains in the queue and isn't returned to subsequent receive requests for the duration of the visibility timeout.
3. Component 2 **deletes** Message A from the queue to prevent the message from being received and processed again once the visibility timeout expires.

Option 1 is because long polling helps reduce the cost of using SQS by eliminating the number of empty responses (when there are no messages available for a ReceiveMessage request) and false empty responses (when messages are available but aren't included in a response). Messages being sent twice in an SQS queue configured with long polling is quite unlikely.

Option 3 is since you are receiving emails from SNS where messages are certainly being processed. Following the scenario, messages not being picked up won't result into 20 messages being sent to your inbox.

Option 4 is because not having the correct permissions would have resulted in a different response. The scenario says that messages were properly processed but there were over 20 messages that were sent, hence, there is no problem with the accessing the queue.

Question 32:

A company is using Redshift for its online analytical processing (OLAP) application which processes complex queries against large datasets. There is a requirement in which you have to define the number of query queues that are available and how queries are routed to those queues for processing.

Which of the following will you use to meet this requirement?

A. This is not possible with Redshift because it is not intended for OLAP application but rather, for OLTP. Use RDS database instead.
B. Create a Lambda function that can accept the number of query queues and use this value to control Redshift.()

C. **Use the workload management (WLM) in the parameter group configuration.(Correct)**
D. This is not possible with Redshift because it is not intended for OLAP application but rather, for OLTP. Use a NoSQL DynamoDB database instead.

Explanation

When you create a parameter group, the default WLM configuration contains one queue that can run up to five queries concurrently. You can add additional queues and configure WLM properties in each of them if you want more control over query processing. Each queue that you add has the same default WLM configuration until you configure its properties. When you add additional queues, the last queue in the configuration is the *default queue*. Unless a query is routed to another queue based on criteria in the WLM configuration, it is processed by the default queue. You cannot specify user groups or query groups for the default queue.

As with other parameters, you cannot modify the WLM configuration in the default parameter group. Clusters associated with the default parameter group always use the default WLM configuration. If you want to modify the WLM configuration, you must create a parameter group and then associate that parameter group with any clusters that require your custom WLM configuration.

Option 3 is correct. In Amazon Redshift, you use workload management (WLM) to define the number of query queues that are available, and how queries are routed to those queues for processing. WLM is part of parameter group configuration. A cluster uses the WLM configuration that is specified in its associated parameter group.

Options 1 and 4 are . Redshift is a good choice if you want to perform OLAP transactions in the cloud. On the contrary, RDS and DynamoDB are more suitable for OLTP applications.

Option 2 is since it will be too costly and inefficient to use Lambda. Workload management (WLM) is a feature of Redshift that addresses the problem aptly.

Question 33:
A web application that you developed stores sensitive information on a non-boot, unencrypted Amazon EBS data volume attached to an Amazon EC2 instance. Which of the following ways could provide protection to the sensitive data of your Amazon EBS volume?

A. Create a new snapshot of the current Amazon EBS volume. Restore the snapshot to a new, encrypted Amazon EBS volume. Mount the Amazon EBS volume.
B. **Create and mount a new, encrypted Amazon EBS volume. Move the data to the new volume and finally, delete the old Amazon EBS volume. (Correct)**
C. Unmount the EBS volume and then set the encryption attribute to true. Afterwards, re-mount the Amazon EBS volume to the instance.

D. Associate the Amazon EBS volume with your AWS CloudHSM and then remount the Amazon EBS volume.

Explanation

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

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

In this scenario, the EBS volume attached to the instance is already unencrypted. The best way to encrypt the data is to create and mount a new, encrypted Amazon EBS volume. Then move the data to the new volume and finally, delete the old, unencrypted Amazon EBS volume. Hence, Option 2 is the correct answer.

Option 1 is because a step is missing for this option to be a valid answer. You need to copy the snapshot first while applying encryption parameters, in order for the resulting target snapshot to be encrypted before restoring it to a new encrypted EBS volume.

Option 3 is because you cannot encrypt the volume even if you unmount the volume. Remember that encryption has to be done during volume creation.

Option 4 is because you cannot create an encrypted snapshot of an unencrypted volume or change existing volume from unencrypted to encrypted. You have to create new encrypted volume and transfer data to the new volume.

Question 34:
You are working as a Solutions Architect for a major telecommunications company where you are assigned to improve the security of your database tier by tightly managing the data flow of your Amazon Redshift cluster. One of the requirements is to use VPC flow logs to monitor all the COPY and UNLOAD traffic of your Redshift cluster that moves in and out of your VPC.

Which of the following is the most suitable solution to implement in this scenario?

A. Use the Amazon Redshift Spectrum feature.
B. Enable Enhanced VPC routing on your Amazon Redshift cluster.(Correct)
C. Enable Audit Logging in your Amazon Redshift cluster.
D. Create a new flow log that tracks the traffic of your Amazon Redshift cluster.

Explanation

When you use Amazon Redshift Enhanced VPC Routing, Amazon Redshift forces all COPY and UNLOAD traffic between your cluster and your data repositories through your Amazon VPC. By using Enhanced VPC Routing, you can use standard VPC features, such as VPC security groups, network access control lists (ACLs), VPC endpoints, VPC endpoint policies, internet gateways, and Domain Name System (DNS) servers. Hence, Option 2 is the correct answer.

You use these features to tightly manage the flow of data between your Amazon Redshift cluster and other resources. When you use Enhanced VPC Routing to route traffic through your VPC, you can also use VPC flow logs to monitor COPY and UNLOAD traffic. If Enhanced VPC Routing is not enabled, Amazon Redshift routes traffic through the Internet, including traffic to other services within the AWS network.

Option 1 is because the Audit Logging feature is primarily used to get the information about the connection, queries, and user activities in your Redshift cluster.

Option 3 is because the Redshift Spectrum is primarily used to run queries against exabytes of unstructured data in Amazon S3, with no loading or ETL required.

Option 4 is because, by default, you cannot create a flow log for your Amazon Redshift cluster. You have to enable Enhanced VPC Routing and set up the required VPC configuration.

Question 35:
A content management system (CMS) is hosted on a fleet of auto-scaled, On-Demand EC2 instances which use Amazon Aurora as its database. Currently, the system stores the file documents that the users uploaded in one of the attached EBS Volumes. Your manager noticed that the system performance is quite slow and he has instructed you to improve the architecture of the system.

In this scenario, what will you do to implement a scalable, high throughput POSIX-compliant file system?

A. Create an S3 bucket and use this as the storage for the CMS
B. Use EFS(Correct)
C. Upgrade your existing EBS volumes to Provisioned IOPS SSD Volumes
D. Use ElastiCache

Explanation

Amazon Elastic File System (Amazon EFS) provides simple, scalable, elastic file storage for use with AWS Cloud services and on-premises resources. When mounted on Amazon EC2 instances, an Amazon EFS file system provides a standard file system interface and file system access semantics, allowing you to seamlessly integrate Amazon EFS with your existing applications and tools. Multiple Amazon EC2 instances can access an Amazon EFS file system at the same time, allowing Amazon EFS to

provide a common data source for workloads and applications running on more than one Amazon EC2 instance.

This particular scenario tests your understanding of EBS, EFS, and S3. In this scenario, there is a fleet of On-Demand EC2 instances that stores file documents from the users to one of the attached EBS Volumes. The system performance is quite slow because the architecture doesn't provide the EC2 instances a parallel shared access to the file documents.

Remember that an EBS Volume can be attached to one EC2 instance at a time, hence, no other EC2 instance can connect to that EBS Provisioned IOPS Volume. Take note as well that the type of storage needed here is a "file storage" which means that S3 (Option 1) is not the best service to use because it is mainly used for "object storage", and S3 does not provide the notion of "folders" too. This is why Option 2 is the correct answer.

Option 3 is because the scenario requires you to set up a scalable, high throughput storage system that will allow concurrent access from multiple EC2 instances. This is clearly not possible in EBS, even with Provisioned IOPS SSD Volumes. You have to use EFS instead.

Option 4 is because ElastiCache is an in-memory data store that improves the performance of your applications, which is not what you need since it is not a file storage.

Question 36:
You are an AWS Solutions Architect designing an online analytics application that uses Redshift Cluster for its data warehouse. Which service will allow you to monitor all API calls to your Redshift instance and can also provide secured data for auditing and compliance purposes?

- **A. CloudTrail for security logs(Correct)**
- B. CloudWatch
- C. AWS X-Ray()
- D. Redshift Spectrum

Explanation

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure.

CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, API calls, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.

Option 2 is because although CloudWatch is also a monitoring service, it cannot track the API calls to your AWS resources.

Option 3 is because AWS X-Ray is not a suitable service to use to track each API call to your AWS resources. It just helps you debug and analyze your microservices applications with request tracing so you can find the root cause of issues and performance.

Option 4 is because Redshift Spectrum is not a monitoring service but rather a feature of Amazon Redshift that enables you to query and analyze all of your data in Amazon S3 using the open data formats you already use, with no data loading or transformations needed.

Question 37:
A popular social network is hosted in AWS and is using a DynamoDB table as its database. There is a requirement to implement a 'follow' feature where users can subscribe to certain updates made by a particular user and be notified via email. Which of the following is the most suitable solution that you should implement to meet the requirement?

A. Using the Kinesis Client Library (KCL), write an application that leverages on DynamoDB Streams Kinesis Adapter that will fetch data from the DynamoDB Streams endpoint. When there are updates made by a particular user, notify the subscribers via email using SNS.
B. Create a Lambda function that uses DynamoDB Streams Kinesis Adapter which will fetch data from the DynamoDB Streams endpoint. Set up an SNS Topic that will notify the subscribers via email when there is an update made by a particular user.
C. Set up a DAX cluster to access the source DynamoDB table. Create a new DynamoDB trigger and a Lambda function. For every update made in the user data, the trigger will send data to the Lambda function which will then notify the subscribers via email using SNS.
D. Enable DynamoDB Stream and create an AWS Lambda trigger, as well as the IAM role which contains all of the permissions that the Lambda function will need at runtime. The data from the stream record will be processed by the Lambda function which will then publish a message to SNS Topic that will notify the subscribers via email.(Correct)

Explanation

A *DynamoDB stream* is an ordered flow of information about changes to items in an Amazon DynamoDB table. When you enable a stream on a table, DynamoDB captures information about every modification to data items in the table.

Whenever an application creates, updates, or deletes items in the table, DynamoDB Streams writes a stream record with the primary key attribute(s) of the items that were modified. A *stream record* contains information about a data modification to a single item in a DynamoDB table. You can configure the stream so that the stream records capture additional information, such as the "before" and "after" images of modified items.

Amazon DynamoDB is integrated with AWS Lambda so that you can create *triggers*—pieces of code that automatically respond to events in DynamoDB Streams. With triggers, you can build applications that react to data modifications in DynamoDB tables.

If you enable DynamoDB Streams on a table, you can associate the stream ARN with a Lambda function that you write. Immediately after an item in the table is modified, a new record appears in the table's stream. AWS Lambda polls the stream and invokes your Lambda function synchronously when it detects new stream records. The Lambda function can perform any actions you specify, such as sending a notification or initiating a workflow. Hence, the correct answer in this scenario is Option 4.

Option 1 is because although this is a valid solution, it is missing a vital step which is to enable DynamoDB Streams. With the DynamoDB Streams Kinesis Adapter in place, you can begin developing applications via the KCL interface, with the API calls seamlessly directed at the DynamoDB Streams endpoint. Remember that the DynamoDB Stream feature is not enabled by default.

Option 2 is because just like Option 1, you have to manually enable DynamoDB Streams first before you can use its endpoint.

Option 3 is because the DynamoDB Accelerator (DAX) feature is primarily used to significantly improve the in-memory read performance of your database, and not to capture the time-ordered sequence of item-level modifications. You should use DynamoDB Streams in this scenario instead.

Question 38:

A media company has an Amazon ECS Cluster, which uses the Fargate launch type, to host its news website. The database credentials should be supplied using environment variables, to comply with strict security compliance. As the Solutions Architect, you have to ensure that the credentials are secure and that they cannot be viewed in plaintext on the cluster itself.

Which of the following is the most suitable solution in this scenario that you can implement with minimal effort?

A. In the ECS task definition file of the ECS Cluster, store the database credentials using Docker Secrets to centrally manage these sensitive data and securely transmit it to only those containers that need access to it. Secrets are encrypted during transit and at rest. A given secret is only accessible to those services which have been granted explicit access to it via IAM Role, and only while those service tasks are running.()

B. Store the database credentials in the ECS task definition file of the ECS Cluster and encrypt it with KMS. Store the task definition JSON file in a private S3 bucket and ensure that HTTPS is enabled on the bucket to encrypt the data in-flight. Create an IAM role to the ECS task definition script that allows access to the specific S3 bucket and then pass the --cli-input-jsonparameter when calling the ECS register-task-definition. Reference the task definition JSON file in the S3 bucket which contains the database credentials.
C. Use the AWS Secrets Manager to store the database credentials and then encrypt them using AWS KMS. Create an IAM Role for your Amazon ECS task execution role and reference it with your task definition which allows access to both KMS and AWS Secrets Manager. Within your container definition, specify secrets with the name of the environment variable to set in the container and the full ARN of the Secrets Manager secret which contains the sensitive data, to present to the container.
D. Use the AWS Systems Manager Parameter Store to keep the database credentials and then encrypt them using AWS KMS. Create an IAM Role for your Amazon ECS task execution role and reference it with your task definition, which allows access to both KMS and the Parameter Store. Within your container definition, specify secrets with the name of the environment variable to set in the container and the full ARN of the Systems Manager Parameter Store parameter containing the sensitive data to present to the container.(Correct)

Explanation

Amazon ECS enables you to inject sensitive data into your containers by storing your sensitive data in either AWS Secrets Manager secrets or AWS Systems Manager Parameter Store parameters and then referencing them in your container definition.

For tasks that use the Fargate launch type, the only supported method is referencing a Systems Manager Parameter Store parameter. This feature also requires that your task use platform version 1.3.0 or later.

For tasks that use the EC2 launch type, both the Secrets Manager secret and Systems Manager Parameter Store parameter methods described are supported. This feature requires that your container instance have version 1.22.0 or later of the container agent. However, it is recommended to use the latest container agent version.

Within your container definition, specify secrets with the name of the environment variable to set in the container and the full ARN of either the Secrets Manager secret or Systems Manager Parameter Store parameter containing the sensitive data to present to the container. The parameter that you reference can be from a different Region than the container using it, but must be from within the same account. Hence, Option 4 is the correct answer.

Option 1 is because although you can use Docker Secrets to secure the sensitive database credentials, this feature is only applicable in Docker Swarm. In AWS, the

recommended way to secure sensitive data is either through the use of Secrets Manager or Systems Manager Parameter Store.

Option 2 is because although the solution may work, it is not recommended to store sensitive credentials in S3. This entails a lot of overhead and manual configuration steps which can be simplified by simply using the Secrets Manager or Systems Manager Parameter Store.

Option 3 is because although the use of Secrets Manager in securing sensitive data in ECS is valid, the use of Secrets Manager is only applicable for EC2 launch type and not for the ones which use a Fargate launch type. The scenario says that the ECS cluster uses a Fargate launch type where the only supported method is referencing the Systems Manager Parameter Store parameter.

Question 39:
A cryptocurrency trading platform is using an API built in AWS Lambda and API Gateway. Due to the recent news and rumors about the upcoming price surge of Bitcoin, Ethereum and other cryptocurrencies, it is expected that the trading platform would have a significant increase in site visitors and new users in the coming days ahead.

In this scenario, how can you protect the backend systems of the platform from traffic spikes?

A. Switch from using AWS Lambda and API Gateway to a more scalable and highly available architecture using EC2 instances, ELB, and Auto Scaling.
B. Enable throttling limits and result caching in API Gateway. (Correct)
C. Use CloudFront in front of the API Gateway to act as a cache.
D. Move the Lambda function in a VPC.

Explanation

Amazon API Gateway provides throttling at multiple levels including global and by service call. Throttling limits can be set for standard rates and bursts. For example, API owners can set a rate limit of 1,000 requests per second for a specific method in their REST APIs, and also configure Amazon API Gateway to handle a burst of 2,000 requests per second for a few seconds. Amazon API Gateway tracks the number of requests per second. Any request over the limit will receive a 429 HTTP response. The client SDKs generated by Amazon API Gateway retry calls automatically when met with this response. Hence, Option 2 is the correct answer.

You can add caching to API calls by provisioning an Amazon API Gateway cache and specifying its size in gigabytes. The cache is provisioned for a specific stage of your APIs. This improves performance and reduces the traffic sent to your back end. Cache settings allow you to control the way the cache key is built and the time-to-live (TTL) of the data stored for each method. Amazon API Gateway also exposes management APIs that help you invalidate the cache for each stage.

Option 1 is since there is no need to transfer your applications to other services.

Option 3 is because CloudFront only speeds up content delivery which provides a better latency experience for your users. It does not help much for the backend.

Option 4 is because this answer is irrelevant to what is being asked. A VPC is your own virtual private cloud where you can launch AWS services.

Question 40:
You are working as a Solutions Architect in a top software development company in Silicon Valley. The company has multiple applications hosted in their VPC. While you are monitoring the system, you noticed that multiple port scans are coming in from a specific IP address block which are trying to connect to several AWS resources inside your VPC. The internal security team has requested that all offending IP addresses be denied for the next 24 hours for security purposes.

Which of the following is the best method to quickly and temporarily deny access from the specified IP addresses?

A. Create a policy in IAM to deny access from the IP Address block. ()
B. Modify the Network Access Control List associated with all public subnets in the VPC to deny access from the IP Address block. (Correct)
C. Add a rule in the Security Group of the EC2 instances to deny access from the IP Address block.
D. Configure the firewall in the operating system of the EC2 instances to deny access from the IP address block.

Explanation

To control the traffic coming in and out of your VPC network, you can use the *network access control list (ACL).* It 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. This is the best solution among other options as you can easily add and remove the restriction in a matter of minutes.

Option 1 is as an IAM policy does not control the inbound and outbound traffic of your VPC.

Option 3 is as although a Security Group acts as a firewall, it will only control both inbound and outbound traffic at the instance level and not on the whole VPC.

Option 4 is because adding a firewall in the underlying operating system of the EC2 instance is not enough; the attacker can just connect to other AWS resources since the network access control list still allows them to do so.

Question 41:

Your cloud architecture is composed of Linux and Windows EC2 instances which process high volumes of financial data 24 hours a day, 7 days a week. To ensure high availability of your systems, you are required to monitor the memory and disk utilization of all of your instances.

Which of the following is the most suitable monitoring solution to implement?

A. Use the default CloudWatch configuration to your EC2 instances where the memory and disk utilization metrics are already available. Install the AWS Systems Manager (SSM) Agent to all of your EC2 instances.
B. Install the CloudWatch agent to all of your EC2 instances which gathers the memory and disk utilization data. View the custom metrics in the Amazon CloudWatch console.(Correct)
C. Enable the Enhanced Monitoring option in EC2 and install CloudWatch agent to all of your EC2 instances to be able to view the memory and disk utilization in the CloudWatch dashboard.
D. Use Amazon Inspector and install the Inspector agent to all of your EC2 instances.

Explanation

CloudWatch has available Amazon EC2 Metrics for you to use for monitoring CPU utilization, Network utilization, Disk performance, and Disk Reads/Writes. In case that you need to monitor the below items, you need to prepare a custom metric using a Perl or other shell script, as there are no ready to use metrics for these:

1. Memory utilization
2. disk swap utilization
3. disk space utilization
4. page file utilization
5. log collection

Take note that there is a multi-platform CloudWatch agent which can be installed on both Linux and Windows-based instances. You can use a single agent to collect both system metrics and log files from Amazon EC2 instances and on-premises servers. This agent supports both Windows Server and Linux and enables you to select the metrics to be collected, including sub-resource metrics such as per-CPU core. It is recommended that you use the new agent instead of the older monitoring scripts to collect metrics and logs.

Option 1 is because, by default, CloudWatch does not automatically provide memory and disk utilization metrics of your instances. You have to set up custom CloudWatch metrics to monitor the memory, disk swap, disk space and page file utilization of your instances.

Option 3 is because Enhanced Monitoring is a feature of RDS and not of CloudWatch.

Option 4 is because Amazon Inspector is an automated security assessment service that helps you test the network accessibility of your Amazon EC2 instances and the security state of your applications running on the instances. It does not provide a custom metric to track the memory and disk utilization of each and every EC2 instance in your VPC.

Question 42:
You are working for a software company that has moved a legacy application from an on-premises data center to the cloud. The legacy application requires a static IP address hard-coded into the backend, which blocks you from using an Application Load Balancer.

Which steps would you take to apply high availability and fault tolerance to this application without ELB?

- **A. Write a script that checks the health of the EC2 instance. If the instance stops responding, the script will switch the elastic IP address to a standby EC2 instance. (Correct)**
- **B. Assign an Elastic IP address to the instance. (Correct)**
- C. Postpone the deployment until you have fully converted the application to work with the ELB and Auto Scaling.
- D. Launch the instance using Auto Scaling which will deploy the instance again if it becomes unhealthy.
- E. Use CloudFront with a custom origin pointed to your on-premises network where the web application is deployed.

Explanation

For this scenario, it is best to set up a self-monitoring EC2 instance with a virtual IP Address. You can use an Elastic IP and then write a custom script that checks the health of the EC2 instance and if the instance stops responding, the script will switch the Elastic IP address to a standby EC2 instance.

A custom script enables one Amazon Elastic Compute Cloud (EC2) instance to monitor another Amazon EC2 instance and take over a private "virtual" IP address on instance failure. When used with two instances, the script enables a High Availability scenario where instances monitor each other and take over a shared virtual IP address if the other instance fails. It could easily be modified to run on a third-party monitoring or witness server to perform the VIP swapping on behalf of the two monitored nodes.

Option 3 is because you don't have to postpone your deployment as you have the option to set up a self-monitoring EC2 instance with an EIP address.

Option 4 is as even though the Auto Scaling group provides high availability and scalability, it still depends on ELB which is not available in this scenario. Take note that you need to have a static IP address which can be in the form of an Elastic IP. Although an Auto Scaling group can scale out if one of the EC2 instances became unhealthy, you

still cannot directly assign an EIP to an Auto Scaling group. In addition, you are only limited to use EC2 instance status checks for your Auto Scaling group if you do not have an ELB which can provide you the actual health check of your application (*using its port*), and not just the health of the EC2 instance.

Option 5 is because although this option is feasible, the goal of the company is to move the application to the cloud and not to continue using its on-premises resources.

Question 43:
A web application is using CloudFront to distribute their images, videos, and other static contents stored in their S3 bucket to its users around the world. The company has recently introduced a new member-only access to some of its high quality media files. There is a requirement to provide access to multiple private media files only to their paying subscribers without having to change their current URLs.

Which of the following is the most suitable solution that you should implement to satisfy this requirement?

A. Configure your CloudFront distribution to use Match Viewer as its Origin Protocol Policy which will automatically match the user request. This will allow access to the private content if the request is a paying member and deny it if it is not a member.
B. Create a Signed URL with a custom policy which only allows the members to see the private files.
C. Configure your CloudFront distribution to use Field-Level Encryption to protect your private data and only allow access to members.
D. Use Signed Cookies to control who can access the private files in your CloudFront distribution by modifying your application to determine whether a user should have access to your content. For members, send the required Set-Cookie headers to the viewer which will unlock the content only to them.(Correct)

Explanation

CloudFront signed URLs and signed cookies provide the same basic functionality: they allow you to control who can access your content. If you want to serve private content through CloudFront and you're trying to decide whether to use signed URLs or signed cookies, consider the following:

Use **signed URLs** for the following cases:

- -You want to use an RTMP distribution. Signed cookies aren't supported for RTMP distributions.
- -You want to restrict access to individual files, for example, an installation download for your application.

- -Your users are using a client (for example, a custom HTTP client) that doesn't support cookies.

Use **signed cookies** for the following cases:

- -You want to provide access to multiple restricted files, for example, all of the files for a video in HLS format or all of the files in the subscribers' area of a website.
- -You don't want to change your current URLs.

Hence, the correct answer to this scenario is Option 4.

Option 1 is because a Match Viewer is an Origin Protocol Policy which configures CloudFront to communicate with your origin using HTTP or HTTPS, depending on the protocol of the viewer request. CloudFront caches the object only once even if viewers make requests using both HTTP and HTTPS protocols.

Option 2 is because Signed URLs are primarily used for providing access to individual files, as shown on the above explanation. In addition, the scenario explicitly says that they don't want to change their current URLs which is why implementing Signed Cookies is more suitable than Signed URL.

Option 3 is because Field-Level Encryption only allows you to securely upload user-submitted sensitive information to your web servers. It does not provide access to download multiple private files.

Question 44:
You have triggered the creation of a snapshot of your EBS volume and is currently on-going. At this point, what are the things that the EBS volume can or cannot do?

A. The volume can be used as normal while the snapshot is in progress.(Correct)
B. The volume can be used in write-only mode while the snapshot is in progress.
C. The volume can be used in read-only mode while the snapshot is in progress.
D. The volume cannot be used until the snapshot completes.

Explanation

EBS snapshots occur asynchronously which makes option 1 the correct answer. This means that the point-in-time snapshot is created immediately, but the status of the snapshot is pending until the snapshot is complete (when all of the modified blocks have been transferred to Amazon S3), which can take several hours for large initial snapshots or subsequent snapshots where many blocks have changed. While it is completing, an in-progress snapshot is not affected by ongoing reads and writes to the volume hence, you can still use the volume.

Option 2, 3 and 4 are because you will still be able to perform normal read and write operations on your EBS volume even while a snapshot is ongoing. Although you can take a snapshot of a volume while a previous snapshot of that volume is in the pending status, having multiple pending snapshots of a volume may result in reduced volume performance until the snapshots complete.

Question 45:
A startup based in Australia is deploying a new two-tier web application in AWS. The Australian company wants to store their most frequently used data in an in-memory data store to improve the retrieval and response time of their web application.

Which of the following is the most suitable service to be used for this requirement?

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

Explanation

Amazon ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory data store or cache in the cloud. The service improves the performance of web applications by allowing you to retrieve information from fast, managed, in-memory data stores, instead of relying entirely on slower disk-based databases.

Option 1 is because DynamoDB is primarily used as a NoSQL database which supports both document and key-value store models. ElastiCache is a more suitable service to use than DynamoDB, if you need an in-memory data store.

Option 2 is because RDS is mainly used as a relational database and not as a data storage for frequently used data.

Option 4 is because Redshift is a data warehouse service and is not suitable to be used as an in-memory data store.

Question 46:
You are designing a multi-tier web application architecture that consists of a fleet of EC2 instances and an Oracle relational database server. It is required that the database is highly available and that you have full control over its underlying operating system.

Which AWS service will you use for your database tier?

A. Amazon RDS
B. Amazon RDS with Multi-AZ deployments

C. Amazon EC2 instances with data replication in one Availability Zone()
D. Amazon EC2 instances with data replication between two different Availability Zones(Correct)

Explanation

To achieve this requirement, you can deploy your Oracle database to Amazon EC2 instances with data replication between two different Availability Zones. Hence, option 4 is the correct answer. The deployment of this architecture can easily be achieved by using Cloudformation and Quick Start. Please refer to the reference link for information.

The Quick Start deploys the Oracle primary database (using the preconfigured, general-purpose starter database from Oracle) on an Amazon EC2 instance in the first Availability Zone. It then sets up a second EC2 instance in a second Availability Zone, copies the primary database to the second instance by using the DUPLICATE command, and configures Oracle Data Guard.

Options 1 and 2 are because the scenario requires you to have access to the underlying operating system of the database server. Remember that Amazon RDS is a managed database service, which means that Amazon is the one that manages the underlying operating system of the database instance and not you.

Option 3 is since deploying to just one Availability Zone (AZ) will not make the database tier highly available. If that AZ went down, your database will be unavailable.

Question 47:
You have a new e-commerce web application written in Angular framework which is deployed to a fleet of EC2 instances behind an Application Load Balancer. You configured the load balancer to perform health checks on these EC2 instances.

What will happen if one of these EC2 instances failed the health checks?

A. The EC2 instance gets terminated automatically by the Application Load Balancer.
B. The EC2 instance gets quarantined by the Application Load Balancer for root cause analysis.
C. The EC2 instance is replaced automatically by the Application Load Balancer.()
D. The Application Load Balancer stops sending traffic to the instance that failed its health check.(Correct)

Explanation

In case that one of the EC2 instances failed a health check, the Application Load Balancer stops sending traffic to that instance.

Your Application Load Balancer periodically sends requests to its registered targets to test their status. These tests are called *health checks*. Each load balancer node routes

requests only to the healthy targets in the enabled Availability Zones for the load balancer. Each load balancer node checks the health of each target, using the health check settings for the target group with which the target is registered. After your target is registered, it must pass one health check to be considered healthy. After each health check is completed, the load balancer node closes the connection that was established for the health check.

Question 48:

A suite of web applications is composed of several different Auto Scaling group of EC2 instances which is configured with default settings and then deployed across three Availability Zones. There is an Application Load Balancer that forwards the request to the respective target group on the URL path. The scale-in policy has been triggered due to the low number of incoming traffic to the application.

Which EC2 instance will be the first one to be terminated by your Auto Scaling group?

A. The EC2 instance which has the least number of user sessions
B. The EC2 instance which has been running for the longest time
C. The EC2 instance which belongs to an Auto Scaling group with the oldest launch configuration (Correct)
D. The instance will be randomly selected by the Auto Scaling group

Explanation

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

1. If there are instances in multiple Availability Zones, choose the Availability Zone with the most instances and at least one instance that is not protected from scale in. If there is more than one Availability Zone with this number of instances, choose the Availability Zone with the instances that use the oldest launch configuration.

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

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

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

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

Question 49:
You are building a new data analytics application in AWS which will be deployed in an Auto Scaling group of On-Demand EC2 instances and a MongoDB database. It is expected that the database will have high-throughput workloads performing small, random I/O operations. As the Solutions Architect, you are required to properly set up and launch the required resources in AWS.

Which of the following is the most suitable EBS type to use for your database?

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

Explanation

On a given volume configuration, certain I/O characteristics drive the performance behavior for your EBS volumes. SSD-backed volumes, such as General Purpose SSD (gp2) and Provisioned IOPS SSD (io1), deliver consistent performance whether an I/O operation is random or sequential. HDD-backed volumes like Throughput Optimized HDD (st1) and Cold HDD (sc1) deliver optimal performance only when I/O operations are large and sequential.

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.

Provisioned IOPS SSD (io1) volumes are designed to meet the needs of I/O-intensive workloads, particularly database workloads, that are sensitive to storage performance and consistency. Unlike gp2, which uses a bucket and credit model to calculate performance, an io1 volume allows you to specify a consistent IOPS rate when you create the volume, and Amazon EBS delivers within 10 percent of the provisioned IOPS performance 99.9 percent of the time over a given year.

	Solid-State Drives (SSD)		Hard Disk Drives (HDD)	
Volume Type	General Purpose SSD (gp2)*	Provisioned IOPS SSD (io1)	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Description	General purpose SSD volume that balances price and performance for a wide variety of workloads	Highest-performance SSD volume for mission-critical low-latency or high-throughput workloads	Low-cost HDD volume designed for frequently accessed, throughput-intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloads
Use Cases	• Recommended for most workloads • System boot volumes • Virtual desktops • Low-latency interactive apps • Development and test environments	• Critical business applications that require sustained IOPS performance, or more than 16,000 IOPS or 250 MiB/s of throughput per volume • Large database workloads, such as: ◦ MongoDB ◦ Cassandra ◦ Microsoft SQL Server ◦ MySQL ◦ PostgreSQL ◦ Oracle	• Streaming workloads requiring consistent, fast throughput at a low price • Big data • Data warehouses • Log processing • Cannot be a boot volume	• Throughput-oriented storage for large volumes of data that is infrequently accessed • Scenarios where the lowest storage cost is important • Cannot be a boot volume
API Name	gp2	io1	st1	sc1
Volume Size	1 GiB - 16 TiB	4 GiB - 16 TiB	500 GiB - 16 TiB	500 GiB - 16 TiB
Max. IOPS/Volume**	16,000***	64,000****	500	250
Max. Throughput/Volume	250 MiB/s***	1,000 MiB/s†	500 MiB/s	250 MiB/s
Max. IOPS/Instance††	80,000	80,000	80,000	80,000
Max. Throughput/Instance††	1,750 MiB/s	1,750 MiB/s	1,750 MiB/s	1,750 MiB/s
Dominant Performance Attribute	IOPS	IOPS	MiB/s	MiB/s

Option 1 is because although General Purpose is a type of SSD that can handle small, random I/O operations, the Provisioned IOPS SSD volumes are much more suitable to meet the needs of I/O-intensive database workloads such as MongoDB, Oracle, MySQL, and many others.

Options 3 and 4 are because HDD volumes (such as Throughput Optimized HDD and Cold HDD volumes) are more suitable for workloads with large, sequential I/O operations instead of small, random I/O operations.

Question 50:
You have launched a travel photo sharing website using Amazon S3 to serve high-quality photos to visitors of your website. After a few days, you found out that there are other travel websites linking and using your photos. This resulted in financial losses for your business.

What is an effective method to mitigate this issue?

A. **Configure your S3 bucket to remove public read access and use pre-signed URLs with expiry dates.(Correct)**
B. Use CloudFront distributions for your photos.
C. Block the IP addresses of the offending websites using NACL.()
D. Store photos on an Amazon EBS volume of the web server.

Explanation

In Amazon S3, all objects are private by default. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL, using their own security credentials, to grant time-limited permission to download the objects.

When you create a pre-signed URL for your object, you must provide your security credentials, specify a bucket name, an object key, specify the HTTP method (GET to download the object) and expiration date and time. The pre-signed URLs are valid only for the specified duration.

Anyone who receives the pre-signed URL can then access the object. For example, if you have a video in your bucket and both the bucket and the object are private, you can share the video with others by generating a pre-signed URL.

Option 2 is . CloudFront is a content delivery network service that speeds up delivery of content to your customers.

Option 3 is also . Blocking IP address using NACLs is not a very efficient method because a quick change in IP address would easily bypass this configuration.

Option 4 is also . You cannot serve objects directly from an EBS volume, which needs to be attached to an EC2 instance. EBS volumes also do not provide the same durability as compared to S3.

Question 51:

A Forex trading platform, which frequently processes and stores global financial data every minute, is hosted in your on-premises data center and uses an Oracle database. Due to a recent cooling problem in their data center, the company urgently needs to migrate their infrastructure to AWS to improve the performance of their applications. As the Solutions Architect, you are responsible in ensuring that the database is properly migrated and should remain available in case of database server failure in the future.

Which of the following is the most suitable solution to meet the requirement?

A. Launch an Oracle database instance in RDS with Recovery Manager (RMAN) enabled.
B. Launch an Oracle Real Application Clusters (RAC) in RDS.()
C. Create an Oracle database in RDS with Multi-AZ deployments. (Correct)
D. Migrate your Oracle data to Amazon Aurora by converting the database schema using AWS Schema Conversion Tool and AWS Database Migration Service.

Explanation

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

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

In this scenario, the best RDS configuration to use is an Oracle database in RDS with Multi-AZ deployments to ensure high availability even if the primary database instance goes down. Hence, Option 3 is the correct answer.

Options 1 and 2 are because Oracle RMAN and RAC are not supported in RDS.

Option 4 is because although this solution is feasible, it takes time to migrate your Oracle database to Aurora which is not acceptable. Based on this option, the Aurora database does not have a Read Replica and is not configured as an Amazon Aurora DB cluster, which could have improved the availability of the database.

Question 52:
A multi-tiered application hosted in your on-premises data center is scheduled to be migrated to AWS. The application has a message broker service which uses industry standard messaging APIs and protocols that must be migrated as well, without rewriting the messaging code in your application.

Which of the following is the most suitable service that you should use to move your messaging service to AWS?

- **A. Amazon MQ(Correct)**
- B. Amazon SQS
- C. Amazon SNS()
- D. Amazon SWF

Explanation

Amazon MQ, Amazon SQS, and Amazon SNS are messaging services that are suitable for anyone from startups to enterprises. If you're using messaging with existing applications and want to move your messaging service to the cloud quickly and easily, it is recommended that you consider Amazon MQ. It supports industry-standard APIs and protocols so you can switch from any standards-based message broker to Amazon MQ without rewriting the messaging code in your applications. Hence, Option 1 is the correct answer.

If you are building brand new applications in the cloud, then it is highly recommended that you consider Amazon SQS and Amazon SNS. Amazon SQS and SNS are lightweight, fully managed message queue and topic services that scale almost infinitely and provide simple, easy-to-use APIs. You can use Amazon SQS and SNS to decouple and scale microservices, distributed systems, and serverless applications, and improve reliability.

Option 2 is because although Amazon SQS is a fully managed message queuing service, it does not support an extensive list of industry-standard messaging APIs and protocol, unlike Amazon MQ. Moreover, using Amazon SQS requires you to do additional changes in the messaging code of applications to make it compatible.

Option 3 is because SNS is more suitable as a pub/sub messaging service instead of a message broker service.

Option 4 is because SWF is a fully-managed state tracker and task coordinator service and not a messaging service, unlike Amazon MQ, AmazonSQS and Amazon SNS.

Question 53:
You are using a combination of API Gateway and Lambda for the web services of your online web portal that is being accessed by hundreds of thousands of clients each day. Your company will be announcing a new revolutionary product and it is expected that your web portal will receive a massive number of visitors all around the globe. How can you protect your backend systems and applications from traffic spikes?

A. **Use throttling limits in API Gateway(Correct)**
B. API Gateway will automatically scale and handle massive traffic spikes so you do not have to do anything.
C. Manually upgrade the EC2 instances being used by API Gateway()
D. Deploy Multi-AZ in API Gateway with Read Replica

Explanation

Amazon API Gateway provides throttling at multiple levels including global and by a service call. Throttling limits can be set for standard rates and bursts. For example, API owners can set a rate limit of 1,000 requests per second for a specific method in their REST APIs, and also configure Amazon API Gateway to handle a burst of 2,000 requests per second for a few seconds.

Amazon API Gateway tracks the number of requests per second. Any requests over the limit will receive a 429 HTTP response. The client SDKs generated by Amazon API Gateway retry calls automatically when met with this response.

Option 2 is because although it can scale using AWS Edge locations, you still need to configure the throttling to further manage the bursts of your APIs.

Option 3 is because API Gateway is a fully managed service and hence, you do not have access to its underlying resources.

Option 4 is because RDS has Multi-AZ and Read Replica capabilities, and not API Gateway.

Question 54:
An online shopping platform is hosted on an Auto Scaling group of Spot EC2 instances and uses Amazon Aurora PostgreSQL as its database. There is a requirement to optimize your database workloads in your cluster where you have to direct production traffic to your high-capacity instances and point the reporting queries sent by your internal staff to the low-capacity instances.

Which is the most suitable configuration for your application as well as your Aurora database cluster to achieve this requirement?

A. Configure your application to use the reader endpoint for both production traffic and reporting queries, which will enable your Aurora database to automatically perform load-balancing among all the Aurora Replicas.
B. In your application, use the cluster endpoint of your Aurora database to handle the incoming production traffic and use the instance endpoint to handle reporting queries.
C. Create a new custom endpoint in Aurora which will load-balance database connections based on the specified criteria. Configure your application to use the custom endpoint for both production traffic and reporting queries. (Correct)
D. In your application, use the writer endpoint of your Aurora database to handle the production traffic. Create a new custom endpoint to handle reporting queries.

Explanation

Amazon Aurora typically involves a cluster of DB instances instead of a single instance. Each connection is handled by a specific DB instance. When you connect to an Aurora cluster, the host name and port that you specify point to an intermediate handler called an *endpoint*. Aurora uses the endpoint mechanism to abstract these connections. Thus, you don't have to hardcode all the hostnames or write your own logic for load-balancing and rerouting connections when some DB instances aren't available.

For certain Aurora tasks, different instances or groups of instances perform different roles. For example, the primary instance handles all data definition language (DDL) and data manipulation language (DML) statements. Up to 15 Aurora Replicas handle read-only query traffic.

Using endpoints, you can map each connection to the appropriate instance or group of instances based on your use case. For example, to perform DDL statements you can connect to whichever instance is the primary instance. To perform queries, you can connect to the reader endpoint, with Aurora automatically performing load-balancing among all the Aurora Replicas. For clusters with DB instances of different capacities or configurations, you can connect to custom endpoints associated with different subsets

of DB instances. For diagnosis or tuning, you can connect to a specific instance endpoint to examine details about a specific DB instance.

The custom endpoint provides load-balanced database connections based on criteria other than the read-only or read-write capability of the DB instances. For example, you might define a custom endpoint to connect to instances that use a particular AWS instance class or a particular DB parameter group. Then you might tell particular groups of users about this custom endpoint. For example, you might direct internal users to low-capacity instances for report generation or ad hoc (one-time) querying, and direct production traffic to high-capacity instances. Hence, Option 3 is the correct answer.

Option 1 is because although it is true that a reader endpoint enables your Aurora database to automatically perform load-balancing among all the Aurora Replicas, it is quite limited to doing read operations only. You still need to use a custom endpoint to load-balance the database connections based on the specified criteria.

Option 2 is because a cluster endpoint (also known as a writer endpoint) for an Aurora DB cluster simply connects to the current primary DB instance for that DB cluster. This endpoint is the only one that can perform write operations in the database such as DDL statements, which is perfect for handling production traffic but not suitable for handling queries for reporting. This kind of endpoint does not have the functionality to automatically perform load-balancing among all the Aurora Replicas of your cluster.

Option 4 is because although this configuration may work, it is not the most suitable option since you can just use one custom endpoint instead of using a separate writer/cluster endpoint to handle the production traffic.

Question 55:
You are a Solutions Architect in your company working with 3 DevOps Engineers under you. One of the engineers accidentally deleted a file hosted in Amazon S3 which has caused disruption of service.

What can you do to prevent this from happening again?
A. Use S3 Infrequently Accessed storage to store the data.

B. Enable S3 Versioning and Multi-Factor Authentication Delete on the bucket. (Correct)

C. Set up a signed URL for all users.()

D. Create an IAM bucket policy that disables delete operation.**Explanation**

To avoid accidental deletion in Amazon S3 bucket, you can:

- Enable Versioning

- Enable MFA (Multi-Factor Authentication) Delete

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures.

If the MFA (Multi-Factor Authentication) Delete is enabled, it requires additional authentication for either of the following operations:

- Change the versioning state of your bucket
- Permanently delete an object version

Option 1 is . Switching your storage class to S3 Infrequent Access won't help mitigate accidental deletions.

Option 3 is . Signed URLs give you more control over access to your content, so this feature deals more on accessing rather than deletion.

Option 4 is . If you create a bucket policy preventing deletion, other users won't be able to delete objects that should be deleted. You only want to prevent accidental deletion, not disable the action itself.

Question 56:
There are a lot of outages in the Availability Zone of your RDS database instance to the point that you have lost access to the database. What could you do to prevent losing access to your database in case that this event happens again?

A. Make a snapshot of the database
B. Enabled Multi-AZ failover(Correct)
C. Increase the database instance size()
D. Create a read replica

Explanation

Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances, making them a natural fit for production database workloads. For this scenario, option 2 is correct. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable.

In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby (or to a read replica in the case of Amazon Aurora), so that you can resume database operations as soon as the failover is complete.

In option 1, creating a snapshot allows you to have a backup of your database, but it does not provide immediate availability in case of AZ failure. So this is .

For option 3, increasing database instance size is not a solution for this problem. Doing this action addresses the need to upgrade your compute capacity but does not solve the requirement of providing access to your database even in the event of a loss of one of the Availability Zones.

Option 4 is because read replicas provide enhanced performance for read-heavy database workloads. Although you can promote a read replica, its asynchronous replication might not provide you the latest version of your database.

Question 57:
You are working for a large financial company as an IT consultant. Your role is to help their development team to build a highly available web application using stateless web servers. In this scenario, which AWS services are suitable for storing session state data?

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

Explanation

Options 2 and 4 are the correct answers. You can store session state data on both DynamoDB and ElastiCache. These AWS services provide high-performance storage of key-value pairs which can be used to build a highly available web application.

Option 1 is since Redshift Spectrum is a data warehousing solution where you can directly query data from your data warehouse. Redshift is not suitable for storing session state, but more on analytics and OLAP processes.

Option 3 is as well since RDS is a relational database solution of AWS. This relational storage type might not be the best fit for session states, and it might not provide the performance you need compared to DynamoDB for the same cost.

Option 5 is as well since Glacier is a low-cost cloud storage service for data archiving and long-term backup. The archival and retrieval speeds of Glacier is too slow for handling session states.

Question 58:
A popular social media website uses a CloudFront web distribution to serve their static contents to their millions of users around the globe. They are receiving a number of complaints recently that their users take a lot of time to log into their website. There are also occasions when their users are getting HTTP 504 errors. You are instructed by your manager to significantly reduce the user's login time to further optimize the system.

Which of the following options should you use together to set up a cost-effective solution that can improve your application's performance? (Choose 2)

A. **Customize the content that the CloudFront web distribution delivers to your users using Lambda@Edge, which allows your Lambda functions to execute the authentication process in AWS locations closer to the users.(Correct)**
B. Use multiple and geographically disperse VPCs to various AWS regions then create a transit VPC to connect all of your resources. In order to handle the requests faster, set up Lambda functions in each region using the AWS Serverless Application Model (SAM) service.
C. Configure your origin to add a Cache-Control max-age directive to your objects, and specify the longest practical value for max-age to increase the cache hit ratio of your CloudFront distribution.
D. Deploy your application to multiple AWS regions to accommodate your users around the world. Set up a Route 53 record with latency routing policy to route incoming traffic to the region that provides the best latency to the user.
E. **Set up an origin failover by creating an origin group with two origins. Specify one as the primary origin and the other as the second origin which CloudFront automatically switches to when the primary origin returns specific HTTP status code failure responses.(Correct)**

Explanation

Lambda@Edge lets you run Lambda functions to customize the content that CloudFront delivers, executing the functions in AWS locations closer to the viewer. The functions run in response to CloudFront events, without provisioning or managing servers. You can use Lambda functions to change CloudFront requests and responses at the following points:

- -After CloudFront receives a request from a viewer (viewer request)
- -Before CloudFront forwards the request to the origin (origin request)
- -After CloudFront receives the response from the origin (origin response)
- -Before CloudFront forwards the response to the viewer (viewer response)

In the given scenario, you can use Lambda@Edge to allow your Lambda functions to customize the content that CloudFront delivers and to execute the authentication process in AWS locations closer to the users. In addition, you can set up an origin failover by creating an origin group with two origins with one as the primary origin and the other as the second origin which CloudFront automatically switches to when the primary origin fails. This will alleviate the occasional HTTP 504 errors that users are experiencing. Therefore, the correct answers are Options 1 and 5.

Option 2 is because of the same reason provided in Option 1 above. Although setting up multiple VPCs across various regions which are connected with a transit VPC is valid, this solution still entails higher setup and maintenance costs. A more cost-effective option would be to use Lambda@Edge instead.

Option 3 is because improving the cache hit ratio for the CloudFront distribution is irrelevant in this scenario. You can improve your cache performance by increasing the proportion of your viewer requests that are served from CloudFront edge caches instead of going to your origin servers for content. However, take note that the problem in the scenario is the sluggish authentication process of your global users and not just the caching of the static objects.

Option 4 is because although this may resolve the performance issue, this solution entails a significant implementation cost since you have to deploy your application to multiple AWS regions. Remember that the scenario asks for a solution that will improve the performance of the application with **minimal cost**.

Question 59:

You have a new joiner in your organization. You have provisioned an IAM user for the new employee in AWS however, the user is not able to perform any actions. What could be the reason for this?

A. IAM users are created by default with partial permissions
B. IAM users are created by default with full permissions
C. IAM users are created by default with no permissions(Correct)
D. You need to wait for 24 hours for the new IAM user to have access.()

Explanation

The reason for this issue is that IAM users are created with no permissions by default. That means that when you created the new IAM user, you might not provisioned any permissions to the user. Hence, option 3 is correct and conversely, options 1 and 2 are wrong.

Option 4 is because provisions are applied immediately, and not after 24 hours.

The IAM user might need to make API calls or use the AWS CLI or the Tools for Windows PowerShell. In that case, create an access key (an access key ID and a secret access key) for that user. This is called Programmatic access.

If the user needs to access AWS resources from the AWS Management Console, create a password and provide it to the user.

Question 60:
Your company announced that there would be a surprise IT audit on all of the AWS resources being used in the production environment. During the audit activities, it was noted that you are using a Reserved EC2 instance on one of your applications. They argued that you should have used Spot EC2 instances instead as it is cheaper than the Reserved Instance.

Which of the following are the characteristics and benefits of using a standard Reserved EC2 instance, which you can use as justification? (Choose 2)

A. Standard Reserved Instances can be later exchanged for other Convertible Reserved Instances
B. You cannot modify the Availability Zone, scope, network platform or instance size.()
C. It can be applied to instances launched by Auto Scaling.(Correct)
D. It runs in a VPC on hardware that's dedicated to a single customer.
E. It provides you with a significant discount compared to On-Demand instance pricing(Correct)

Explanation

Reserved Instances (RIs) provide you with a significant discount (up to 75%) compared to On-Demand instance pricing. You have the flexibility to change families, OS types, and tenancies while benefiting from RI pricing when you use Convertible RIs. One important thing to remember here is that Reserved Instances are notphysical instances, but rather a billing discount applied to the use of On-Demand Instances in your account.

When your computing needs change, you can modify your Standard or Convertible Reserved Instances and continue to take advantage of the billing benefit. You can modify the Availability Zone, scope, network platform, or instance size (within the same instance type) of your Reserved Instance. You can also sell your unused instance on the Reserved Instance Marketplace.

Option 1 is because only Convertible Reserved Instances can be exchanged for other Convertible Reserved Instances.

Option 2 is because you can indeed modify the Availability Zone, scope, network platform, or instance size of your Reserved Instance as long as it is within the same instance type.

Option 3 is correct because you can definitely use Auto Scaling on Reserved Instances. Remember that it is basically just a billing concept hence, you can use features like

Auto Scaling with your Reserved Instances, same as with your Spot and On-Demand instances. Keep in mind that Reserved Instances are not physical servers/instances, but rather a billing discount applied to the use of On-Demand Instances in your account.

Option 4 is wrong because that is the description of a Dedicated instance and not a Reserved Instance. A Dedicated instance runs in a VPC on hardware that's dedicated to a single customer.

Option 5 is correct because reserved instances can be used to lower costs. Reserved Instances provide you with a discount on usage of EC2 instances, and a capacity reservation when they are applied to a specific Availability Zone, giving you additional confidence that you will be able to launch the instances you have reserved when you need them.

Question 61:
You are working as a Solutions Architect for a government project in which they are building an online portal to allow people to pay their taxes and claim their tax refunds online. Due to the confidentiality of data, the security policy requires that the application hosted in EC2 encrypts the data first before writing it to the disk for storage.

In this scenario, which service would you use to meet this requirement?

A. Security Token Service
B. EBS encryption
C. Elastic File System (EFS)()
D. AWS KMS API(Correct)

Explanation

AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. The master keys that you create in AWS KMS are protected by FIPS 140-2 validated cryptographic modules. AWS KMS is integrated with most other AWS services that encrypt your data with encryption keys that you manage. AWS KMS is also integrated with AWS CloudTrail to provide encryption key usage logs to help meet your auditing, regulatory and compliance needs.

In this scenario, you can configure your application to use the KMS API to encrypt all data before saving it to disk. Hence, Option 4 is the correct answer.

Option 1 is because AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for AWS Identity and Access Management (IAM) users or for users that you authenticate (federated users). It is not used for encrypting data unlike KMS.

Option 2 is because although EBS encryption provides additional security for the EBS volumes, the application could not use this service to encrypt or decrypt each individual

data that it writes on the disk. It is better to use KMS API instead to automatically encrypt the data before saving it to disk.

Option 3 is because EFS is a storage service and does not provide encryption services unlike KMS API.

Question 62:
You are working as a Solutions Architect in a new startup that provides storage for high-quality photos which are infrequently accessed by the users. To make the architecture cost-effective, you designed the cloud service to use an S3 One Zone-Infrequent Access (S3 One Zone-IA) storage type for free users and an S3 Standard-Infrequent Access (S3 Standard-IA) storage type for premium users. When your manager found out about this, he asked you about the trade-offs of using S3 One Zone-IA instead of the S3 Standard-IA.

What will you say to your manager?

A. **Unlike other Amazon object storage classes, which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ.(Correct)**
B. **Storing data in S3 One Zone-IA costs less than storing it in S3 Standard-IA.(Correct)**
C. Storing data in S3 One Zone-IA costs more than storing it in S3 Standard-IA but provides more durability.
D. Unlike other Amazon object storage classes, which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in two AZs only. Hence the name, One Zone-IA since the data replication is skipped in one Availability Zone.
E. S3 One Zone-IA offers lower durability and low throughput compared with Amazon S3 Standard and S3 Standard-IA which is why it has a low per GB storage price and per GB retrieval fee.

Explanation

Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) is an Amazon S3 storage class for data that is accessed less frequently but requires rapid access when needed. Unlike other Amazon object storage classes, which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ. Because of this, storing data in S3 One Zone-IA costs 20% less than storing it in S3 Standard-IA. S3 One Zone-IA is ideal for customers who want a lower cost option for infrequently accessed data but do not require the availability and resilience of S3 Standard or S3 Standard-IA storage. It’s a good choice, for example, for storing secondary backup copies of on-premises data or easily re-creatable data, or for storage used as an S3 Cross-Region Replication target from another AWS Region.

S3 One Zone-IA offers the same high durability, high throughput, and low latency of Amazon S3 Standard and S3 Standard-IA, with a low per GB storage price and per GB

retrieval fee. The S3 One Zone-IA storage class is set at the object level and can exist in the same bucket as S3 Standard and S3 Standard-IA, allowing you to use S3 Lifecycle Policies to automatically transition objects between storage classes without any application changes.

Key Features:

- -Same low latency and high throughput performance of S3 Standard and S3 Standard-IA
- -Designed for durability of 99.999999999% of objects in a single Availability Zone, but data will be lost in the event of Availability Zone destruction
- -Designed for 99.5% availability over a given year
- -Backed with the Amazon S3 Service Level Agreement for availability
- -Supports SSL for data in transit and encryption of data at rest
- -Lifecycle management for automatic migration of objects

Remember that since the S3 One Zone-IA stores data in a single AWS Availability Zone, data stored in this storage class will be lost in the event of Availability Zone destruction.

Question 63:
A Docker application, which is running on an Amazon ECS cluster behind a load balancer, is heavily using DynamoDB. You are instructed to improve the database performance by distributing the workload evenly and using the provisioned throughput efficiently.

Which of the following would you consider to implement for your DynamoDB table?

A. Reduce the number of partition keys in the DynamoDB table.
B. Use partition keys with high-cardinality attributes, which have a large number of distinct values for each item.(Correct)
C. Use partition keys with low-cardinality attributes, which have a few number of distinct values for each item.()
D. Avoid using a composite primary key, which is composed of a partition key and a sort key.

Explanation

The partition key portion of a table's primary key determines the logical partitions in which a table's data is stored. This in turn affects the underlying physical partitions. Provisioned I/O capacity for the table is divided evenly among these physical partitions. Therefore a partition key design that doesn't distribute I/O requests evenly can create "hot" partitions that result in throttling and use your provisioned I/O capacity inefficiently.

The optimal usage of a table's provisioned throughput depends not only on the workload patterns of individual items, but also on the partition-key design. This doesn't mean that you must access all partition key values to achieve an efficient throughput level, or even that the percentage of accessed partition key values must be high. It does mean that the more distinct partition key values that your workload accesses, the more those requests will be spread across the partitioned space. In general, you will use your provisioned throughput more efficiently as the ratio of partition key values accessed to the total number of partition key values increases.

One example for this is the use of partition keys with high-cardinality attributes, which have a large number of distinct values for each item. Hence, Option 2 is the correct answer.

Option 1 is because instead of reducing the number of partition keys in your DynamoDB table, you should actually add more to improve its performance to distribute the I/O requests evenly and not avoid "hot" partitions.

Option 3 is because this is the exact opposite of the correct answer. Remember that the more distinct partition key values your workload accesses, the more those requests will be spread across the partitioned space. Conversely, the less distinct partition key values, the less evenly spread it would be across the partitioned space, which effectively slows the performance.

Option 4 is because, just like Option 2, a composite primary key will provide more partition for the table and in turn, improves the performance. Hence, it should be used and not avoided.

Question 64:
You are designing a banking portal which uses Amazon ElastiCache for Redis as its distributed session management component. Since the other Cloud Engineers in your department have access to your ElastiCache cluster, you have to secure the session data in the portal by requiring them to enter a password before they are granted permission to execute Redis commands.

As the Solutions Architect, which of the following should you do to meet the above requirement?

A. Set up an IAM Policy and MFA which requires the Cloud Engineers to enter their IAM credentials and token before they can access the ElastiCache cluster.
B. Set up a Redis replication group and enable the AtRestEncryptionEnabledparameter.
C. Authenticate the users using Redis AUTH by creating a new Redis Cluster with both the --transit-encryption-enabled and --auth-token parameters enabled.(Correct)
- Enable the in-transit encryption for Redis replication groups.

Explanation

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

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

Option 1 is because this is not possible in IAM. You have to use the Redis AUTH option instead.

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

Option 4 is because although in-transit encryption is part of the solution, it is missing the most important thing which is the Redis AUTH option.

Question 65:
You have identified a series of DDoS attacks while monitoring your VPC. As the Solutions Architect, you are responsible in fortifying your current cloud infrastructure to protect the data of your clients.

Which of the following is the most suitable solution to mitigate these kinds of attacks?

A. **Use AWS Shield to detect and mitigate DDoS attacks.(Correct)**
B. Using the AWS Firewall Manager, set up a security layer that will prevent SYN floods, UDP reflection attacks and other DDoS attacks.
C. Set up a web application firewall using AWS WAF to filter, monitor, and block HTTP traffic.()
D. A combination of Security Groups and Network Access Control Lists to only allow authorized traffic to access your VPC.

Explanation

For higher levels of protection against attacks targeting your applications running on Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing(ELB), Amazon CloudFront, and Amazon Route 53 resources, you can subscribe to AWS Shield Advanced. In addition to the network and transport layer protections that come with Standard, AWS Shield Advanced provides additional detection and mitigation against large and sophisticated DDoS attacks, near real-time visibility into attacks, and integration with AWS WAF, a web application firewall.

AWS Shield Advanced also gives you 24x7 access to the AWS DDoS Response Team (DRT) and protection against DDoS related spikes in your Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing(ELB), Amazon CloudFront, and Amazon Route 53 charges.

Option 2 is because the AWS Firewall Manager is mainly used to simplify your AWS WAF administration and maintenance tasks across multiple accounts and resources. It does not protect your VPC against DDoS attacks.

Option 3 is because even though AWS WAF can help you block common attack patterns to your VPC such as SQL injection or cross-site scripting, this is still not enough to withstand DDoS attacks. It is better to use AWS Shield in this scenario.

Option 4 is because although using a combination of Security Groups and NACLs are valid to provide security to your VPC, this is not enough to mitigate a DDoS attack. You should use AWS Shield for better security protection.