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 the storage of their personal documents.

Which of the following will you need to consider so you can set up a solution that incorporates a 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? (Select TWO.)

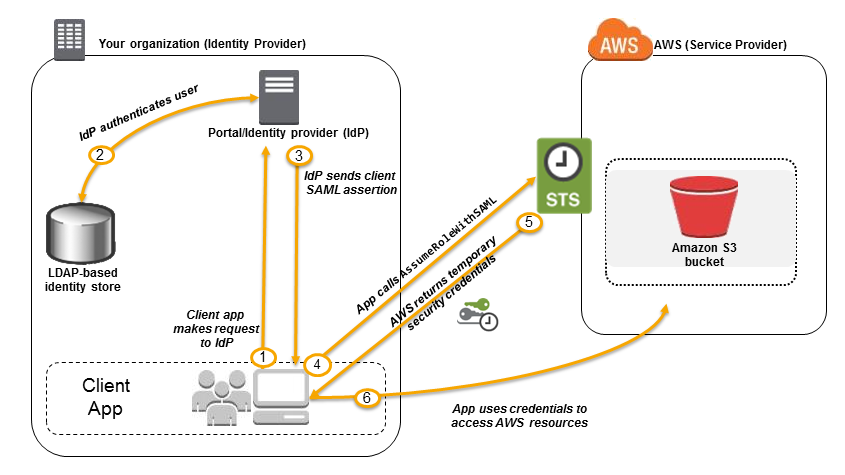
ANS: The question refers to one of the common scenarios for temporary credentials in AWS. Temporary credentials are useful in scenarios that involve identity federation, delegation, cross-account access, and IAM roles. In this example, it is called **enterprise identity federation** considering that 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**

**- Configure an IAM role and an IAM Policy to access the bucket.**



Incorrect: **Mapping each individual user to a designated user folder in S3 using Amazon WorkDocs to access their personal documents** is incorrect as there is no direct way of integrating Amazon S3 with Amazon WorkDocs for this particular scenario. Amazon WorkDocs is simply a fully managed, secure content creation, storage, and collaboration service. With Amazon WorkDocs, you can easily create, edit, and share content. And because it’s stored centrally on AWS, you can access it from anywhere on any device

A company is designing a banking portal that 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?

ANS: 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, the correct answer is: **Authenticate the users using Redis AUTH by creating a new Redis Cluster with both the --transit-encryption-enabled and --auth-token parameters enabled.**

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.

**Amazon CloudWatch** has available Amazon EC2 Metrics for you to use for monitoring CPU utilization, Network utilization, Disk performance, and Disk Reads/Writes. In case 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:

Memory utilization

Disk swap utilization

Disk space utilization

Page file utilization

Log collection

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

ANS: 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.

Incorrect: The option that says: **There is no need to do anything because, by default, AWS Lambda already encrypts the environment variables using the AWS Key Management Service** is incorrect. Although Lambda encrypts the environment variables in your function by default, the sensitive information would still be visible to other users who have access to the Lambda console. This is because Lambda uses a default KMS key to encrypt the variables, which is usually accessible by other users. The best option in this scenario is to use encryption helpers to secure your environment variables.

A company conducted 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 combination of Standard and Convertible Reserved EC2 instances in your applications.

Which of the following are the characteristics and benefits of using these two types of Reserved EC2 instances? (Select TWO.)

ANS: **- Unused Standard Reserved Instances can later be sold at the Reserved Instance Marketplace.**

**- Convertible Reserved Instances allow you to exchange for another convertible reserved instance of a different instance family.**

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?

ANS: **enabling throttling limits and result caching in API Gateway** :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.

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.

Incoreect: **Using CloudFront in front of the API Gateway to act as a cache** is incorrect because CloudFront only speeds up content delivery which provides a better latency experience for your users. It does not help much for the backend.

a file gateway, you can do the following:

- You can store and retrieve files directly using the NFS version 3 or 4.1 protocol.

- You can store and retrieve files directly using the SMB file system version, 2 and 3 protocol.

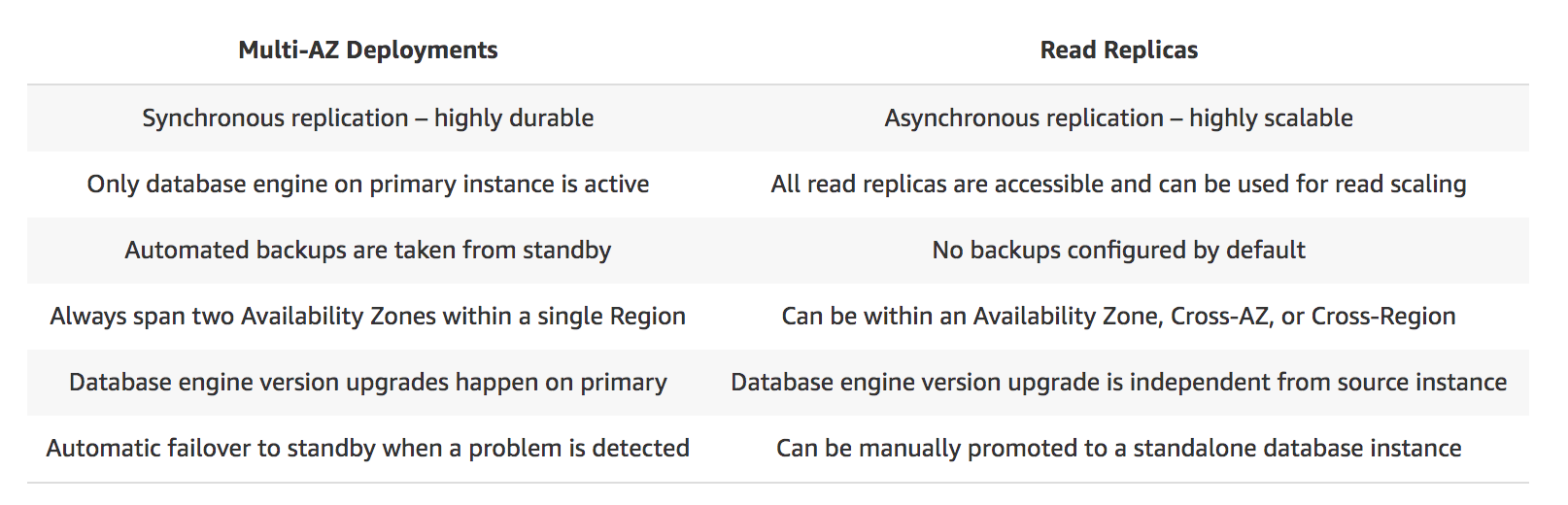
- You can access your data directly in Amazon S3 from any AWS Cloud application or service.

- You can manage your Amazon S3 data using lifecycle policies, cross-region replication, and versioning. You can think of a file gateway as a file system mount on S3.

AWS Storage Gateway supports the Amazon S3 Standard, Amazon S3 Standard-Infrequent Access, Amazon S3 One Zone-Infrequent Access and Amazon Glacier storage classes.

Although you can write objects directly from a file share to the S3-Standard-IA or S3-One Zone-IA storage class, it is recommended that you use a Lifecycle Policy to transition your objects rather than write directly from the file share, especially if you're expecting to update or delete the object within 30 days of archiving it.

 An alternative solution is to use AWS Direct Connect with AWS Storage Gateway to create a connection for high-throughput workload needs, providing a dedicated network connection between your on-premises file gateway and AWS. But this solution is using EBS, hence, this option is still wrong.



An online medical system hosted in AWS stores sensitive Personally Identifiable Information (PII) of the users in an Amazon S3 bucket. Both the master keys and the unencrypted data should never be sent to AWS to comply with the strict compliance and regulatory requirements of the company.

Which S3 encryption technique should the Architect use?

ANS: client side master key

To enable client-side encryption, you have the following options:

- Use an AWS KMS-managed customer master key.

- Use a client-side master key.

When using an AWS KMS-managed customer master key to enable client-side data encryption, you provide an AWS KMS customer master key ID (CMK ID) to AWS. On the other hand, when you use client-side master key for client-side data encryption, your client-side master keys and your unencrypted data are never sent to AWS. It's important that you safely manage your encryption keys because if you lose them, you can't decrypt your data.

This is how client-side encryption using client-side master key works:

**When uploading an object** - You provide a client-side master key to the Amazon S3 encryption client. The client uses the master key only to encrypt the data encryption key that it generates randomly. The process works like this:

1. The Amazon S3 encryption client generates a one-time-use symmetric key (also known as a data encryption key or data key) locally. It uses the data key to encrypt the data of a single Amazon S3 object. The client generates a separate data key for each object.

2. The client encrypts the data encryption key using the master key that you provide. The client uploads the encrypted data key and its material description as part of the object metadata. The client uses the material description to determine which client-side master key to use for decryption.

3. The client uploads the encrypted data to Amazon S3 and saves the encrypted data key as object metadata (x-amz-meta-x-amz-key) in Amazon S3.

**When downloading an object -**The client downloads the encrypted object from Amazon S3. Using the material description from the object's metadata, the client determines which master key to use to decrypt the data key. The client uses that master key to decrypt the data key and then uses the data key to decrypt the object.

Incorrect: **Using S3 server-side encryption with customer provided key** is incorrect because just as mentioned above, you have to use client-side encryption in this scenario instead of server-side encryption. For the S3 server-side encryption with customer-provided key (SSE-C), you actually provide the encryption key as part of your request to upload the object to S3. Using this key, Amazon S3 manages both the encryption (as it writes to disks) and decryption (when you access your objects).

An application is hosted in an AWS Fargate cluster that runs a batch job whenever an object is loaded on an Amazon S3 bucket. The minimum number of ECS Tasks is initially set to 1 to save on costs, and it will only increase the task count based on the new objects uploaded on the S3 bucket. Once processing is done, the bucket becomes empty and the ECS Task count should be back to 1.

Which is the most suitable option to implement with the LEAST amount of effort?

ANS: **Set up a CloudWatch Event rule to detect S3 object PUT operations and set the target to the ECS cluster with the increased number of tasks. Create another rule to detect S3 DELETE operations and set the target to the ECS Cluster with 1 as the Task count.**

**Incorrect: Set up an alarm in CloudWatch to monitor CloudTrail since this S3 object-level operations are recorded on CloudTrail. Set two alarm actions to update ECS task count to scale-out/scale-in depending on the S3 event** is incorrect because you can’t directly set CloudWatch Alarms to update the ECS task count. You have to use CloudWatch Events instead.

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?

ANS: **enabling Enhanced Monitoring in RDS**

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.

A company requires all the data stored in the cloud to be encrypted at rest. To easily integrate this with other AWS services, they must have full control over the encryption of the created keys and also the ability to immediately remove the key material from AWS KMS. The solution should also be able to audit the key usage independently of AWS CloudTrail.

Which of the following options will meet this requirement?

ANS: : **Use AWS Key Management Service to create a CMK in a custom key store and store the non-extractable key material in AWS CloudHSM**

AWS KMS can help you integrate with other AWS services to encrypt the data that you store in these services and control access to the keys that decrypt it. To immediately remove the key material from AWS KMS, you can use a custom key store. Take note that each custom key store is associated with an AWS CloudHSM cluster in your AWS account. Therefore, when you create an AWS KMS CMK in a custom key store, AWS KMS generates and stores the non-extractable key material for the CMK in an AWS CloudHSM cluster that you own and manage. This is also suitable if you want to be able to audit the usage of all your keys independently of AWS KMS or AWS CloudTrail.

Since you control your AWS CloudHSM cluster, you have the option to manage the lifecycle of your CMKs independently of AWS KMS. There are four reasons why you might find a custom key store useful:

You might have keys that are explicitly required to be protected in a single-tenant HSM or in an HSM over which you have direct control.

You might have keys that are required to be stored in an HSM that has been validated to FIPS 140-2 level 3 overall (the HSMs used in the standard AWS KMS key store are either validated or in the process of being validated to level 2 with level 3 in multiple categories).

You might need the ability to immediately remove key material from AWS KMS and to prove you have done so by independent means.

You might have a requirement to be able to audit all use of your keys independently of AWS KMS or AWS CloudTrail.

Incorrect:

The option that says: **Use AWS Key Management Service to create a CMK in a custom key store and store the non-extractable key material in Amazon S3** is incorrect because Amazon S3 is not a suitable storage service to use in storing encryption keys. You have to use AWS CloudHSM instead.

The options that say: **Use AWS Key Management Service to create AWS-owned CMKs and store the non-extractable key material in AWS CloudHSM**and **Use AWS Key Management Service to create AWS-managed CMKs and store the non-extractable key material in AWS CloudHSM** are both incorrect because the scenario requires you to have full control over the encryption of the created key. AWS-owned CMKs and AWS-managed CMKs are managed by AWS. Moreover, these options do not allow you to audit the key usage independently of AWS CloudTrail.

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 the write operations of the 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?

ANS: **creating a custom endpoint in Aurora based on the specified criteria for the production traffic and another custom endpoint to handle the reporting queries**

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

A company needs to design an online analytics application that uses Redshift Cluster for its data warehouse. Which of the following services allows them to monitor all API calls in Redshift instance and can also provide secured data for auditing and compliance purposes?

ANS: **AWS CloudTrail** is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account

Incorrect: **AWS X-Ray** is incorrect because this 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.

**Amazon CloudWatch** is incorrect. Although this is also a monitoring service, it cannot track the API calls to your AWS resources.

A car dealership website hosted in Amazon EC2 stores car listings in an Amazon Aurora database managed by Amazon RDS. Once a vehicle has been sold, its data must be removed from the current listings and forwarded to a distributed processing system.

Which of the following options can satisfy the given requirement?

ANS:  **Create a native function or a stored procedure that invokes a Lambda function. Configure the Lambda function to send event notifications to an Amazon SQS queue for the processing system to consume.** You can invoke an AWS Lambda function from an Amazon Aurora MySQL-Compatible Edition DB cluster with a native function or a stored procedure. This approach can be useful when you want to integrate your database running on Aurora MySQL with other AWS services. In the scenario, you can trigger a Lambda function whenever a listing is deleted from the database. You can then write the logic of the function to send the listing data to an SQS queue and have different processes consume it.

A Solutions Architect is working for a company which has multiple VPCs in various AWS regions. The Architect is assigned to set up a logging system which will track all of the changes made to their AWS resources in all regions, including the configurations made in IAM, CloudFront, AWS WAF, and Route 53. In order to pass the compliance requirements, the solution must ensure the security, integrity, and durability of the log data. It should also provide an event history of all API calls made in AWS Management Console and AWS CLI.

Which of the following solutions is the best fit for this scenario?

ANS: **Set up a new CloudTrail trail in a new S3 bucket using the AWS CLI and also pass both the --is-multi-region-trail and --include-global-service-events parameters then encrypt log files using KMS encryption. Apply Multi Factor Authentication (MFA) Delete on the S3 bucket and ensure that only authorized users can access the logs by configuring the bucket policies** is correct because it provides security, integrity, and durability to your log data and in addition, it has the -include-global-service-events parameter enabled which will also include activity from global services such as IAM, Route 53, AWS WAF, and CloudFront.

There are two types of events that can be logged in CloudTrail: management events and data events. By default, trails log management events, but not data events. A trail can be applied to all regions or a single region. As a best practice, create a trail that applies to all regions in the AWS partition in which you are working. This is the default setting when you create a trail in the CloudTrail console.

In this scenario, the company requires a secure and durable logging solution that will track all of the activities of all AWS resources in all regions. CloudTrail can be used for this case with multi-region trail enabled, however, it will only cover the activities of the regional services (EC2, S3, RDS etc.) and not for global services such as IAM, CloudFront, AWS WAF, and Route 53. In order to satisfy the requirement, you have to add the --include-global-service-events parameter in your AWS CLI command.

INCORRECT:  **Set up a new CloudWatch trail in a new S3 bucket using the AWS CLI and also pass both the --is-multi-region-trail and --include-global-service-events parameters then encrypt log files using KMS encryption. Apply Multi Factor Authentication (MFA) Delete on the S3 bucket and ensure that only authorized users can access the logs by configuring the bucket policies** is incorrect because you need to use CloudTrail instead of CloudWatch.

A startup is using Amazon RDS to store data from a web application. Most of the time, the application has low user activity but it receives bursts of traffic within seconds whenever there is a new product announcement. The Solutions Architect needs to create a solution that will allow users around the globe to access the data using an API.

What should the Solutions Architect do meet the above requirement?

ANS: **Create an API using Amazon API Gateway and use AWS Lambda to handle the bursts of traffic.** Based on the given scenario, you need to create a solution that will satisfy the two requirements. The first requirement is to create a solution that will allow the users to access the data using an API. To implement this solution, you can use Amazon API Gateway. The second requirement is to handle the burst of traffic within seconds. You should use AWS Lambda in this scenario because Lambda functions can absorb reasonable bursts of traffic for approximately 15-30 minutes.

Lambda can scale faster than the regular Auto Scaling feature of Amazon EC2, Amazon Elastic Beanstalk, or Amazon ECS. This is because AWS Lambda is more lightweight than other computing services.

A pharmaceutical company 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?

ANS: **Set up SAML 2.0-Based Federation by using a Microsoft Active Directory Federation Service (AD FS).**

**Incorrect: Setting up SAML 2.0-Based Federation by using a Web Identity Federation** is incorrect because this 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.

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?

ANS: **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 (taskRoleArn) 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**.

Secrets can be exposed to a container in the following ways:

- To inject sensitive data into your containers as environment variables, use the secrets container definition parameter.

- To reference sensitive information in the log configuration of a container, use the secretOptions container definition parameter.

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.

INCORRECT: The option that says: **Use the AWS Secrets Manager to store the database credentials and then encrypt them using AWS KMS. Create a resource-based policy for your Amazon ECS task execution role (taskRoleArn) 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** is incorrect. Although the use of Secrets Manager in securing sensitive data in ECS is valid, Amazon ECS doesn't support resource-based policies. An example of a resource-based policy is the S3 bucket policy. An ECS task assumes an execution role (IAM role) to be able to call other AWS services like AWS Secrets Manager on your behalf.

A financial application is composed of an Auto Scaling group of EC2 instances, an Application Load Balancer, and a MySQL RDS instance in a Multi-AZ Deployments configuration. To protect the confidential data of your customers, you have to 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?

ANS: **enabling IAM DB Authentication**

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

INCORRECT: **Creating an IAM Role and assigning it to your EC2 instances which will grant exclusive access to your RDS instance** is incorrect 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.

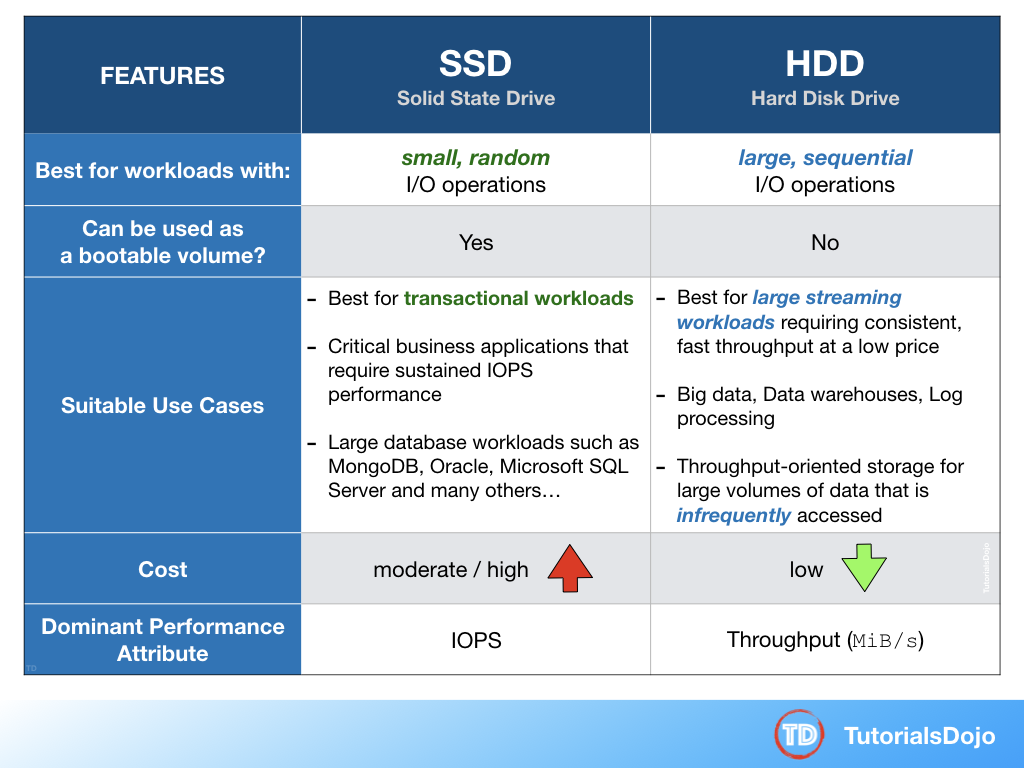
A company plans to build a data analytics application in AWS which will be deployed in an Auto Scaling group of On-Demand EC2 instances and a MongoDB database. It is expected that the database will have high-throughput workloads performing small, random I/O operations. As the Solutions Architect, you 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?

ANS: Provisioned IOPS SSD (io1/io2)

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.

INCORRECT: **General Purpose SSD (gp2)** is incorrect 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.



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

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

An organization is currently using a tape backup solution to store its application data on-premises. They plan to use a cloud storage service to preserve the backup data for up to 10 years that may be accessed about once or twice a year.

Which of the following is the most cost-effective option to implement this solution?

ANS: Tape Gateway encrypts data between the gateway and AWS for secure data transfer and compresses data and transitions virtual tapes between Amazon S3 and Amazon S3 Glacier, or Amazon S3 Glacier Deep Archive, to minimize storage costs.

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

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

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

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

Hence, **increasing the write capacity assigned to the shard table** is the correct answer.

A digital media company shares static content to its premium users around the world and also to their partners who syndicate their media files. The company is looking for ways to reduce its server costs and securely deliver their data to their customers globally with low latency.

Which combination of services should be used to provide the MOST suitable and cost-effective architecture? (Select TWO.)

ANS: **Amazon CloudFront** and **Amazon S3.**

**INCORRECT: AWS Global Accelerator** is incorrect because this service is more suitable for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover. Moreover, there is no direct way that you can integrate AWS Global Accelerator with Amazon S3. It's more suitable to use Amazon CloudFront instead in this scenario.

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

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

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

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

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

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

**Incorrect**: The option that says: The **record set must be of type "MX"** is incorrect since an MX record specifies the mail server responsible for accepting email messages on behalf of a domain name. This is not what is being asked by the question.

The option that says: The **S3 bucket must be in the same region as the hosted zone** is incorrect. There is no constraint that the S3 bucket must be in the same region as the hosted zone in order for the Route 53 service to route traffic into it.

The option that says: **The Cross-Origin Resource Sharing (CORS) option should be enabled in the S3 bucket** is incorrect because you only need to enable Cross-Origin Resource Sharing (CORS) when your client web application on one domain interacts with the resources in a different domain.

A software company has resources hosted in AWS and on-premises servers. You have been requested to create a decoupled architecture for applications which make use of both resources.  
  
Which of the following options are valid? (Select TWO.)

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

Incorrect: **Using VPC peering to connect both on-premises servers and EC2 instances for your decoupled application** is incorrect because you can't create a VPC peering for your on-premises network and AWS VPC.

An organization needs to control the access for several S3 buckets. They plan to use a gateway endpoint to allow access to trusted buckets.

Which of the following could help you achieve this requirement?

ANS: **Generate an endpoint policy for trusted S3 buckets.**

A **VPC endpoint** enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.

When you create a VPC endpoint, you can attach an endpoint policy that controls access to the service to which you are connecting. You can modify the endpoint policy attached to your endpoint and add or remove the route tables used by the endpoint. An endpoint policy does not override or replace IAM user policies or service-specific policies (such as S3 bucket policies). It is a separate policy for controlling access from the endpoint to the specified service.

We can use a bucket policy or an endpoint policy to allow the traffic to trusted S3 buckets. The options that have 'trusted S3 buckets' key phrases will be the possible answer in this scenario. It would take you a lot of time to configure a bucket policy for each S3 bucket instead of using a single endpoint policy. Therefore, you should use an endpoint policy to control the traffic to the trusted Amazon S3 buckets.

A VPC endpoint policy is an IAM resource policy that you attach to an endpoint when you create or modify the endpoint. If you do not attach a policy when you create an endpoint, we attach a default policy for you that allows full access to the service. If a service does not support endpoint policies, the endpoint allows full access to the service. An endpoint policy does not override or replace IAM user policies or service-specific policies (such as S3 bucket policies). It is a separate policy for controlling access from the endpoint to the specified service.

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

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

ANS: **using Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation of EBS snapshots**

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

- Protect valuable data by enforcing a regular backup schedule.

- Retain backups as required by auditors or internal compliance.

- Reduce storage costs by deleting outdated backups.

Combined with the monitoring features of Amazon CloudWatch Events and AWS CloudTrail, Amazon DLM provides a complete backup solution for EBS volumes at no additional cost.

A company is planning to launch an application which requires a data warehouse that will be used for their infrequently accessed data. You need to use an EBS Volume that can handle large, sequential I/O operations.

Which of the following is the most cost-effective storage type that you should use to meet the requirement?

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

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

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

* 

**It is not possible to allow multiple domains to serve SSL traffic over the same IP address in AWS**

**(Incorrect)**

* 

**Use an Elastic IP and upload multiple 3rd party certificates in your Classic Load Balancer using the AWS Certificate Manager.**

* 

**Use Server Name Indication (SNI) on your Classic Load Balancer by adding multiple SSL certificates to allow multiple domains to serve SSL traffic.**

* 

**Generate an SSL certificate with AWS Certificate Manager and create a CloudFront web distribution. Associate the certificate with your web distribution and enable the support for Server Name Indication (SNI).**

**(Correct)**

**Explanation**

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

A company is using multiple AWS accounts that are consolidated using AWS Organizations. They want to copy several S3 objects to another S3 bucket that belonged to a different AWS account which they also own. The Solutions Architect was instructed to set up the necessary permissions for this task and to ensure that the destination account owns the copied objects and not the account it was sent from.

How can the Architect accomplish this requirement?

ANS: **Configure cross-account permissions in S3 by creating an IAM customer-managed policy that allows an IAM user or role to copy objects from the source bucket in one account to the destination bucket in the other account. Then attach the policy to the IAM user or role that you want to use to copy objects between accounts.**

A company has an existing VPC which is quite unutilized for the past few months. The Business Manager instructed the Solutions Architect to integrate the company’s on-premises data center and its VPC. The architect explained the list of tasks that he’ll be doing and discussed the Virtual Private Network (VPN) connection. The Business Manager is not tech-savvy but he is interested to know what a VPN is and its benefits.

What is one of the major advantages of having a VPN in AWS?

ANS: **It allows you to connect your AWS cloud resources to your on-premises data center using secure and private sessions with IP Security (IPSec) or Transport Layer Security (TLS) tunnels**

**You are automating the creation of EC2 instances in your VPC. Hence, you wrote a python script to trigger the Amazon EC2 API to request 50 EC2 instances in a single Availability Zone. However, you noticed that after 20 successful requests, subsequent requests failed.  
  
What could be a reason for this issue and how would you resolve it?**

**ANS:** You are limited to running On-Demand Instances per your vCPU-based On-Demand Instance limit, purchasing 20 Reserved Instances, and requesting Spot Instances per your dynamic Spot limit per region. New AWS accounts may start with limits that are lower than the limits described here. If you need more instances, complete the Amazon EC2 limit increase request form with your use case, and your limit increase will be considered. Limit increases are tied to the region they were requested for.

In Amazon EC2, you can manage your instances from the moment you launch them up to their termination. You can flexibly control your computing costs by changing the EC2 instance state. Which of the following statements is true regarding EC2 billing? (Select TWO.)

ANS: The option that says: **You will be billed when your On-Demand instance is preparing to hibernate with a stopping state** is correct because when the instance state is **stopping**, you will not billed if it is preparing to stop however, you **will still be billed** if it is just preparing to hibernate.

The option that says: **You will be billed when your Reserved instance is in terminated state** is correct because Reserved Instances that applied to terminated instances are still billed until the end of their term according to their payment option. I actually raised a pull-request to Amazon team about the billing conditions for Reserved Instances, which has been approved and reflected on your official AWS Documentation: <https://github.com/awsdocs/amazon-ec2-user-guide/pull/45>

INCORRECT:

The option that says: **You will be billed when your On-Demand instance is in pending state** is incorrect because you will not be billed if your instance is in **pending** state.

The option that says: **You will be billed when your Spot instance is preparing to stop with a stopping state** is incorrect because you will not be billed if your instance is preparing to stop with a **stopping** state.

The option that says: **You will not be billed for any instance usage while an instance is not in the running state** is incorrect because the statement is not entirely true. You can still be billed if your instance is preparing to hibernate with a **stopping**state.

A FinTech startup deployed an application on an Amazon EC2 instance with attached Instance Store volumes and an Elastic IP address. The server is only accessed from 8 AM to 6 PM and can be stopped from 6 PM to 8 AM for cost efficiency using Lambda with the script that automates this based on tags.

Which of the following will occur when the EC2 instance is stopped and started? (Select TWO.)

ANS: the correct answers are:

**- The underlying host for the instance is possibly changed.**

**- All data on the attached instance-store devices will be lost.**

The option that says: **The ENI (Elastic Network Interface) is detached** is incorrect because the ENI will stay attached even if you stopped your EC2 instance.

The option that says: **The Elastic IP address is disassociated with the instance** is incorrect because the EIP will actually remain associated with your instance even after stopping it.

The option that says: **There will be no changes** is incorrect because there will be a lot of possible changes in your EC2 instance once you stop and start it again. AWS may move the virtualized EC2 instance to another host computer; the instance may get a new public IP address, and the data in your attached instance store volumes will be deleted.

A company is deploying a Microsoft SharePoint Server environment on AWS using CloudFormation. The Solutions Architect needs to install and configure the architecture that is composed of Microsoft Active Directory (AD) domain controllers, Microsoft SQL Server 2012, multiple Amazon EC2 instances to host the Microsoft SharePoint Server and many other dependencies. The Architect needs to ensure that the required components are properly running before the stack creation proceeds.

Which of the following should the Architect do to meet this requirement?

ANS: You can associate the **CreationPolicy** attribute with a resource to prevent its status from reaching create complete until AWS CloudFormation receives a specified number of success signals or the timeout period is exceeded. To signal a resource, you can use the cfn-signal helper script or SignalResource API. AWS CloudFormation publishes valid signals to the stack events so that you track the number of signals sent.

Currently, the only AWS CloudFormation resources that support creation policies are AWS::AutoScaling::AutoScalingGroup, AWS::EC2::Instance, and AWS::CloudFormation::WaitCondition

INCORRECT: The option that says: **Configure the DependsOn attribute in the CloudFormation template. Send a success signal after the applications are installed and configured using the cfn-init helper script** is incorrect because the cfn-init helper script is not suitable to be used to signal another resource. You have to use cfn-signal instead. And although you can use the DependsOn attribute to ensure the creation of a specific resource follows another, it is still better to use the CreationPolicy attribute instead as it ensures that the applications are properly running before the stack creation proceeds.

The option that says: **Configure a UpdatePolicy attribute to the instance in the CloudFormation template. Send a success signal after the applications are installed and configured using the cfn-signal helper script**is incorrect because the UpdatePolicy attribute is primarily used for updating resources and for stack update rollback operations.

A Solutions Architect working for a startup is designing a High Performance Computing (HPC) application which is publicly accessible for their customers. The startup founders want to mitigate distributed denial-of-service (DDoS) attacks on their application.

Which of the following options are not suitable to be implemented in this scenario? (Select TWO.)

ANS: **Using Dedicated EC2 instances to ensure that each instance has the maximum performance possible**

**Adding multiple Elastic Fabric Adapters (EFA) to each EC2 instance to increase the network bandwidth**

The following options are valid mitigation techniques that can be used to prevent DDoS:

**- Use an Amazon CloudFront service for distributing both static and dynamic content.**

**- Use an Application Load Balancer with Auto Scaling groups for your EC2 instances. Prevent direct Internet traffic to your Amazon RDS database by deploying it to a new private subnet.**

**- Use AWS Shield and AWS WAF.**

A large financial firm in the country has an AWS environment that contains several Reserved EC2 instances hosting a web application that has been decommissioned last week. To save costs, you need to stop incurring charges for the Reserved instances as soon as possible.

What cost-effective steps will you take in this circumstance? (Select TWO.)

ANS: Hence, the correct answers are:

**- Go to the AWS Reserved Instance Marketplace and sell the Reserved instances.**

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

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

**Contacting AWS to cancel your AWS subscription** is incorrect as you don't need to close down your AWS account.

**Going to the Amazon.com online shopping website and selling the Reserved instances** is incorrect as you have to use AWS Reserved Instance Marketplace to sell your instances.

A company is setting up a cloud architecture for an international money transfer service to be deployed in AWS which will have thousands of users around the globe. The service should be available 24/7 to avoid any business disruption and should be resilient enough to handle the outage of an entire AWS region. To meet this requirement, the Solutions Architect has deployed their AWS resources to multiple AWS Regions. He needs to use Route 53 and configure it to set all of the resources to be available all the time as much as possible. When a resource becomes unavailable, Route 53 should detect that it's unhealthy and stop including it when responding to queries.

Which of the following is the most fault-tolerant routing configuration that the Solutions Architect should use in this scenario?

* 

**Configure an Active-Passive Failover with Multiple Primary and Secondary Resources.**

**(Incorrect)**

* 

**Configure an Active-Active Failover with Weighted routing policy.**

**(Correct)**

* 

**Configure an Active-Passive Failover with Weighted Records.**

* 

**Configure an Active-Active Failover with One Primary and One Secondary Resource.**

#### ANS: Explanation

You can use **Route 53 health checking** to configure active-active and active-passive failover configurations. You configure active-active failover using any routing policy (or combination of routing policies) other than failover, and you configure active-passive failover using the failover routing policy.

**Active-Active Failover**

Use this failover configuration when you want all of your resources to be available the majority of the time. When a resource becomes unavailable, Route 53 can detect that it's unhealthy and stop including it when responding to queries.

In active-active failover, all the records that have the same name, the same type (such as A or AAAA), and the same routing policy (such as weighted or latency) are active unless Route 53 considers them unhealthy. Route 53 can respond to a DNS query using any healthy record.

**Active-Passive Failover**

Use an active-passive failover configuration when you want a primary resource or group of resources to be available the majority of the time and you want a secondary resource or group of resources to be on standby in case all the primary resources become unavailable. When responding to queries, Route 53 includes only the healthy primary resources. If all the primary resources are unhealthy, Route 53 begins to include only the healthy secondary resources in response to DNS queries.

A Solutions Architect needs to deploy a mobile application that can collect votes for a popular singing competition. Millions of users from around the world will submit votes using their mobile phones. These votes must be collected and stored in a highly scalable and highly available data store which will be queried for real-time ranking.

Which of the following combination of services should the architect use to meet this requirement?

ANS: DYNAMO DB with APP SYNC

#### Explanation

When the word durability pops out, the first service that should come to your mind is Amazon S3. Since this service is not available in the answer options, we can look at the other data store available which is Amazon DynamoDB.

**DynamoDB** is durable, scalable, and highly available data store which can be used for real-time tabulation. You can also use **AppSync** with DynamoDB to make it easy for you to build collaborative apps that keep shared data updated in real time

INCORRECT:

**Amazon Redshift and AWS Mobile Hub** are incorrect as Amazon Redshift is mainly used as a data warehouse and for online analytic processing (OLAP). Although this service can be used for this scenario, DynamoDB is still the top choice given its better durability and scalability.

**Amazon Relational Database Service (RDS) and Amazon MQ** and **Amazon Aurora and Amazon Cognito** are possible answers in this scenario, however, DynamoDB is much more suitable for simple mobile apps that do not have complicated data relationships compared with enterprise web applications. It is stated in the scenario that the mobile app will be used from around the world, which is why you need a data storage service which can be supported globally. It would be a management overhead to implement multi-region deployment for your RDS and Aurora database instances compared to using the Global table feature of DynamoDB.

A company hosted a web application on a Linux Amazon EC2 instance in the public subnet that uses a default network ACL. The instance uses a default security group and has an attached Elastic IP address. The network ACL has been configured to block all traffic to the instance. The Solutions Architect must allow incoming traffic on port 443 to access the application from any source.

Which combination of steps will accomplish this requirement? (Select TWO.)

ANS:  the correct answers are:

**- In the Security Group, add a new rule to allow TCP connection on port 443 from source 0.0.0.0/0.**

**- In the Network ACL, update the rule to allow inbound TCP connection on port 443 from source 0.0.0.0/0 and outbound TCP connection on port 32768 - 65535 to destination 0.0.0.0/0.**

#### Explanation

To enable the connection to a service running on an instance, the associated network ACL must allow both inbound traffic on the port that the service is listening on as well as allow outbound traffic from ephemeral ports. When a client connects to a server, a random port from the ephemeral port range (1024-65535) becomes the client's source port.

The designated ephemeral port then becomes the destination port for return traffic from the service, so outbound traffic from the ephemeral port must be allowed in the network ACL. By default, network ACLs allow all inbound and outbound traffic. If your network ACL is more restrictive, then you need to explicitly allow traffic from the ephemeral port range.

The client that initiates the request chooses the ephemeral port range. The range varies depending on the client's operating system.

- Many Linux kernels (including the Amazon Linux kernel) use ports 32768-61000.

- Requests originating from Elastic Load Balancing use ports 1024-65535.

- Windows operating systems through Windows Server 2003 use ports 1025-5000.

- Windows Server 2008 and later versions use ports 49152-65535.

- A NAT gateway uses ports 1024-65535.

- AWS Lambda functions use ports 1024-65535.

**INCORRECT:**

The option that says:**In the Security Group, create a new rule to allow TCP connection on port 443 to destination 0.0.0.0/0**is incorrect because this step just allows outbound connections from the EC2 instance out to the public Internet which is unnecessary. Remember that a default security group already includes an outbound rule that allows all outbound traffic.

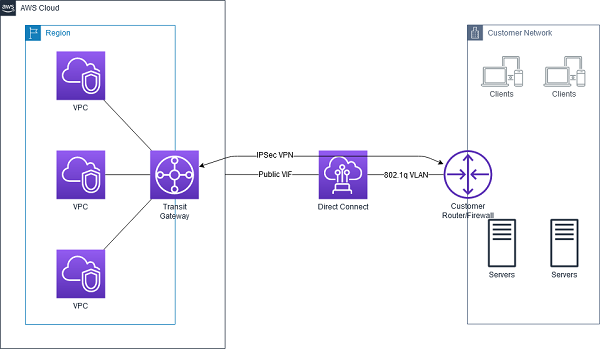
The option that says:**In the Network ACL, update the rule to allow both inbound and outbound TCP connection on port 443 from source 0.0.0.0/0 and to destination 0.0.0.0/0** is incorrect because your network ACL must have an outbound rule to allow ephemeral ports (32768 - 65535). These are the specific ports that will be used as the client's source port for the traffic response.

The option that says:**In the Network ACL, update the rule to allow outbound TCP connection on port 32768 - 65535 to destination 0.0.0.0/0**is incorrect because this step is just partially right. You still need to add an inbound rule from port 443 and not just the outbound rule for the ephemeral ports (32768 - 65535).

A company has established a dedicated network connection from its on-premises data center to AWS Cloud using AWS Direct Connect (DX). The core network services, such as the Domain Name System (DNS) service and Active Directory services, are all hosted on-premises. The company has new AWS accounts that will also require consistent and dedicated access to these network services.

Which of the following can satisfy this requirement with the LEAST amount of operational overhead and in a cost-effective manner?

ANS: **Create a new Direct Connect gateway and integrate it with the existing Direct Connect connection. Set up a Transit Gateway between AWS accounts and associate it with the Direct Connect gateway.**



**INCORRECT:**

The option that says:**Set up another Direct Connect connection for each and every new AWS account that will be added**is incorrect because this solution entails a significant amount of additional cost. Setting up a single DX connection requires a substantial budget and takes a lot of time to establish. It also has high management overhead since you will need to manage all of the Direct Connect connections for all AWS accounts.

The option that says:**Create a new AWS VPN CloudHub. Set up a Virtual Private Network (VPN) connection for additional AWS accounts** is incorrect because a VPN connection is not capable of providing consistent and dedicated access to the on-premises network services. Take note that a VPN connection traverses the public Internet and doesn't use a dedicated connection.

The option that says:**Set up a new Direct Connect gateway and integrate it with the existing Direct Connect connection. Configure a VPC peering connection between AWS accounts and associate it with Direct Connect gateway**is incorrect because VPC peering is not supported in a Direct Connect connection. VPC peering does not support transitive peering relationships.

An application needs to retrieve a subset of data from a large CSV file stored in an Amazon S3 bucket by using simple SQL expressions. The queries are made within Amazon S3 and must only return the needed data.

Which of the following actions should be taken?

ANS: **Perform an S3 Select operation based on the bucket's name and object's key.** You can perform S3 Select to query only the necessary data inside the CSV files based on the bucket's name and the object's key.

INCORRECT: he option that says: **Perform an S3 Select operation based on the bucket's name and object's metadata**is incorrect because metadata is not needed when querying subsets of data in an object using S3 Select.

The option that says: **Perform an S3 Select operation based on the bucket's name and object tags**is incorrect because object tags just provide additional information to your object.

**Perform an S3 Select operation based on the bucket's name**is incorrect because you need both the bucket’s name and the object key to successfully perform an S3 Select operation.

A media company recently launched their newly created web application. Many users tried to visit the website, but they are receiving a 503 Service Unavailable Error. The system administrator tracked the EC2 instance status and saw the capacity is reaching its maximum limit and unable to process all the requests. To gain insights from the application's data, they need to launch a real-time analytics service.

Which of the following allows you to read records in batches?

ANS:  **Create a Kinesis Data Stream and use AWS Lambda to read records from the data stream**.

INCORRECT:

The option that says: **Create a Kinesis Data Firehose and use AWS Lambda to read records from the data stream** is incorrect. Although Amazon Kinesis Data Firehose captures and loads data in near real-time, AWS Lambda can't be set as its destination. You can write Lambda functions and integrate it with Kinesis Data Firehose to request additional, customized processing of the data before it is sent downstream. However, this integration is primarily used for stream processing and not the actual consumption of the data stream. You have to use a Kinesis Data Stream in this scenario.

The options that say: **Create an Amazon S3 bucket to store the captured data and use Amazon Athena to analyze the data** and **Create an Amazon S3 bucket to store the captured data and use Amazon Redshift Spectrum to analyze the data** are both incorrect. As per the scenario, the company needs a real-time analytics service that can ingest and process data. You need to use Amazon Kinesis to process the data in real-time.

A company is storing its financial reports and regulatory documents in an Amazon S3 bucket. To comply with the IT audit, they tasked their Solutions Architect to track all new objects added to the bucket as well as the removed ones. It should also track whether a versioned object is permanently deleted. The Architect must configure Amazon S3 to publish notifications for these events to a queue for post-processing and to an Amazon SNS topic that will notify the Operations team.

Which of the following is the MOST suitable solution that the Architect should implement?

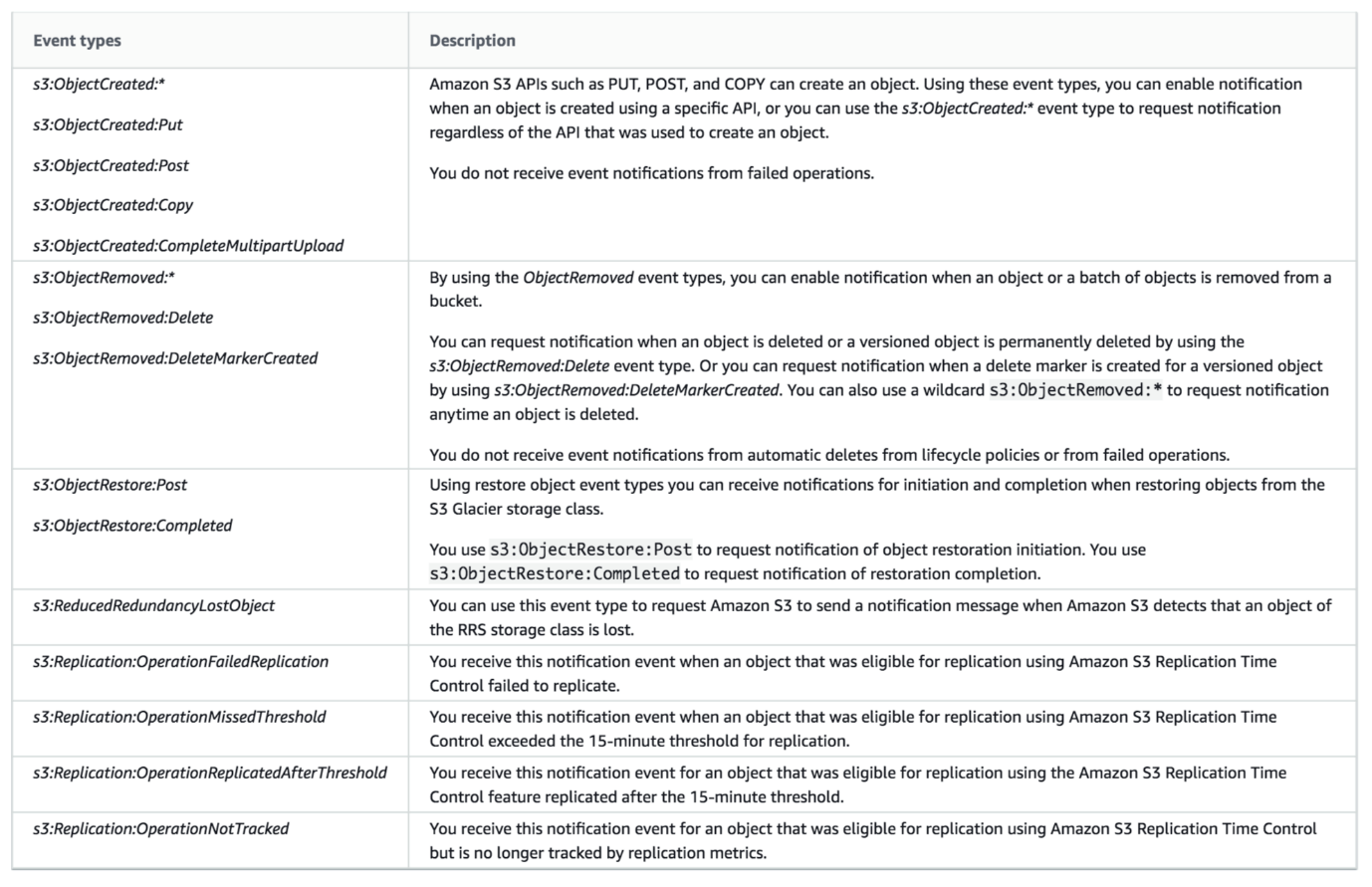
ANS: **Create a new Amazon SNS topic and Amazon SQS queue. Add an S3 event notification configuration on the bucket to publish s3:ObjectCreated:\* and s3:ObjectRemoved:Delete event types to SQS and SNS.**

**INCORRECT:**

The option that says: **Create a new Amazon SNS topic and Amazon MQ. Add an S3 event notification configuration on the bucket to publish s3:ObjectAdded:\* and s3:ObjectRemoved:\* event types to SQS and SNS** is incorrect. There is no s3:ObjectAdded:\* type in Amazon S3**.**You should add an S3 event notification configuration on the bucket to publish events of the s3:ObjectCreated:\* type instead. Moreover, Amazon S3 does support Amazon MQ as a destination to publish events.

The option that says: **Create a new Amazon SNS topic and Amazon SQS queue. Add an S3 event notification configuration on the bucket to publish s3:ObjectCreated:\* and ObjectRemoved:DeleteMarkerCreated event types to SQS and SNS** is incorrect because the s3:ObjectRemoved:DeleteMarkerCreated type is only triggeredwhen a delete marker is created for a versioned object and not when an object is deleted or a versioned object is permanently deleted.

The option that says: **Create a new Amazon SNS topic and Amazon MQ. Add an S3 event notification configuration on the bucket to publish s3:ObjectCreated:\* and ObjectRemoved:DeleteMarkerCreated event types to SQS and SNS** is incorrect because Amazon S3 does public event messages to Amazon MQ. You should use an Amazon SQS instead. In addition, the s3:ObjectRemoved:DeleteMarkerCreated type is only triggeredwhen a delete marker is created for a versioned object. Remember that the scenario asked to publish events when an object is deleted or a versioned object is permanently deleted.



An aerospace engineering company recently adopted a hybrid cloud infrastructure with AWS. One of the Solutions Architect’s tasks is to launch a VPC with both public and private subnets for their EC2 instances as well as their database instances.

Which of the following statements are true regarding Amazon VPC subnets? (Select TWO.)

* 

**The allowed block size in VPC is between a /16 netmask (65,536 IP addresses) and /27 netmask (32 IP addresses).**

* 

**Each subnet maps to a single Availability Zone.**

**(Correct)**

* 

**Each subnet spans to 2 Availability Zones.**

* 

**Every subnet that you create is automatically associated with the main route table for the VPC.**

**(Correct)**

* 

**EC2 instances in a private subnet can communicate with the Internet only if they have an Elastic IP.**

#### Explanation for incorrect:

**EC2 instances in a private subnet can communicate with the Internet only if they have an Elastic IP** is incorrect. EC2 instances in a private subnet can communicate with the Internet not just by having an Elastic IP, but also with a public IP address via a NAT Instance or a NAT Gateway. Take note that there is a distinction between private and public IP addresses. To enable communication with the Internet, a public IPv4 address is mapped to the primary private IPv4 address through network address translation (NAT).

The option that says: **The allowed block size in VPC is between a /16 netmask (65,536 IP addresses) and /27 netmask (32 IP addresses)** is incorrect because the allowed block size in VPC is between a /16 netmask (65,536 IP addresses) and /28 netmask (16 IP addresses) and not /27 netmask.

The option that says: **Each subnet spans to 2 Availability Zones** is incorrect because each subnet must reside entirely within one Availability Zone and cannot span zones.

AWS App Mesh is just a service mesh that provides application-level networking to make it easy for your services to communicate with each other across multiple types of compute infrastructure.

AWS Cloud Map is simply a cloud resource discovery service that enables you to name your application resources with custom names and automatically update the locations of your dynamically changing resources.

The time period from when a record is added to when it is no longer accessible is called the retention period. A Kinesis data stream stores records from **24 hours by default** to a maximum of 168 hours

**In RDS, you still have to manually scale up your resources and create Read Replicas to improve scalability while in DynamoDB, this is automatically done**.

A large telecommunications company needs to run analytics against all combined log files from the Application Load Balancer as part of the regulatory requirements.

Which AWS services can be used together to collect logs and then easily perform log analysis?

* 

**Amazon DynamoDB for storing and EC2 for analyzing the logs.**

* 

**Amazon S3 for storing the ELB log files and an EC2 instance for analyzing the log files using a custom-built application.**

* 

**Amazon EC2 with EBS volumes for storing and analyzing the log files.**

* 

**Amazon S3 for storing ELB log files and Amazon EMR for analyzing the log files.**

**(Correct)**

#### Explanation: log analysis can be automatically provided by Amazon EMR, which is more economical than building a custom-built log analysis application and hosting it in EC2. Hence, the option that says: **Amazon S3 for storing ELB log files and Amazon EMR for analyzing the log files** is the best answer

The option that says: **Amazon DynamoDB for storing and EC2 for analyzing the logs** is incorrect because DynamoDB is a noSQL database solution of AWS. It would be inefficient to store logs in DynamoDB while using EC2 to analyze them.

The option that says: **Amazon EC2 with EBS volumes for storing and analyzing the log files** is incorrect because using EC2 with EBS would be costly, and EBS might not provide the most durable storage for your logs, unlike S3.

The option that says: **Amazon S3 for storing the ELB log files and an EC2 instance for analyzing the log files using a custom-built application** is incorrect because using EC2 to analyze logs would be inefficient and expensive since you will have to program the analyzer yourself.

There is no additional charge for using gateway endpoints. However, standard charges for data transfer and resource usage still apply. However you pay an hourly rate for every provisioned Interface endpoint

A travel company has a suite of web applications hosted in an Auto Scaling group of On-Demand EC2 instances behind an Application Load Balancer that handles traffic from various web domains such as i-love-manila.com, i-love-boracay.com, i-love-cebu.com and many others. To improve security and lessen the overall cost, you are instructed to secure the system by allowing multiple domains to serve SSL traffic without the need to reauthenticate and reprovision your certificate everytime you add a new domain. This migration from HTTP to HTTPS will help improve their SEO and Google search ranking.

Which of the following is the most cost-effective solution to meet the above requirement?

ANS: **Upload all SSL certificates of the domains in the ALB using the console and bind multiple certificates to the same secure listener on your load balancer. ALB will automatically choose the optimal TLS certificate for each client using Server Name Indication (SNI).**

**Incorret:**

**Create a new CloudFront web distribution and configure it to serve HTTPS requests using dedicated IP addresses in order to associate your alternate domain names with a dedicated IP address in each CloudFront edge location** is incorrect because although it is valid to use dedicated IP addresses to meet this requirement, this solution is not cost-effective. Remember that if you configure CloudFront to serve HTTPS requests using dedicated IP addresses, you incur an additional monthly charge. The charge begins when you associate your SSL/TLS certificate with your CloudFront distribution. You can just simply upload the certificates to the ALB and use SNI to handle multiple domains in a cost-effective manner.

A company needs to use Amazon Aurora as the Amazon RDS database engine of their web application. The Solutions Architect has been instructed to implement a 90-day backup retention policy.

Which of the following options can satisfy the given requirement?

* 

**Create an AWS Backup plan to take daily snapshots with a retention period of 90 days.**

**(Correct)**

* 

**Create a daily scheduled event using CloudWatch Events and AWS Lambda to directly download the RDS automated snapshot to an S3 bucket. Archive snapshots older than 90 days to Glacier.**

* 

**Configure RDS to export the automated snapshot automatically to Amazon S3 and create a lifecycle policy to delete the object after 90 days.**

* 

**Configure an automated backup and set the backup retention period to 90 days.**

ANS: **Create an AWS Backup plan to take daily snapshots with a retention period of 90 days.** you can use AWS Backup to create a backup plan with a retention period of 90 days. A backup plan is a policy expression that defines when and how you want to back up your AWS resources. You assign resources to backup plans, and AWS Backup then automatically backs up and retains backups for those resources according to the backup plan.

INCORRECT:

**Configure an automated backup and set the backup retention period to 90 days** is incorrect because the maximum backup retention period for automated backup is only 35 days.

The option that says: **Configure RDS to export the automated snapshot automatically to Amazon S3 and create a lifecycle policy to delete the object after 90 days**is incorrect because you can't export an automated snapshot automatically to Amazon S3. You must export the snapshot manually.

The option that says:**Create a daily scheduled event using CloudWatch Events and AWS Lambda to directly download the RDS automated snapshot to an S3 bucket. Archive snapshots older than 90 days to Glacier** is incorrect because you cannot directly download or export an automated snapshot in RDS to Amazon S3. You have to copy the automated snapshot first for it to become a manual snapshot, which you can move to an Amazon S3 bucket. A better solution for this scenario is to simply use AWS Backup.

An online stocks trading application that stores financial data in an S3 bucket has a lifecycle policy that moves older data to Glacier every month. There is a strict compliance requirement where a surprise audit can happen at anytime and you should be able to retrieve the required data in under 15 minutes under all circumstances. Your manager instructed you to ensure that retrieval capacity is available when you need it and should handle up to 150 MB/s of retrieval throughput.

Which of the following should you do to meet the above requirement? (Select TWO.)

* 

**Use Expedited Retrieval to access the financial data.**

**(Correct)**

* 

**Specify a range, or portion, of the financial data archive to retrieve.**

* 

**Purchase provisioned retrieval capacity.**

**(Correct)**

* 

**Retrieve the data using Amazon Glacier Select.**

* 

**Use Bulk Retrieval to access the financial data.**

ANS: **Expedited retrievals** allow you to quickly access your data when occasional urgent requests for a subset of archives are required. For all but the largest archives (250 MB+), data accessed using Expedited retrievals are typically made available within 1–5 minutes. Provisioned Capacity ensures that retrieval capacity for Expedited retrievals is available when you need it.

 Each unit of capacity provides that at least three expedited retrievals can be performed every five minutes and provides up to 150 MB/s of retrieval throughput. You should purchase provisioned retrieval capacity if your workload requires highly reliable and predictable access to a subset of your data in minutes.

A company has an e-commerce application that saves the transaction logs to an S3 bucket. You are instructed by the CTO to configure the application to keep the transaction logs for one month for troubleshooting purposes, and then afterward, purge the logs.

What should you do to accomplish this requirement?

* 

**Add a new bucket policy on the Amazon S3 bucket.**

* 

**Configure the lifecycle configuration rules on the Amazon S3 bucket to purge the transaction logs after a month**

**(Correct)**

* 

**Create a new IAM policy for the Amazon S3 bucket that automatically deletes the logs after a month**

* 

**Enable CORS on the Amazon S3 bucket which will enable the automatic monthly deletion of data**

ANS: Lifecycle configuration enables you to specify the lifecycle management of objects in a bucket. The configuration is a set of one or more rules, where each rule defines an action for Amazon S3 to apply to a group of objects. These actions can be classified as follows:

**Transition actions** – In which you define when objects transition to another storage class. For example, you may choose to transition objects to the STANDARD\_IA (IA, for infrequent access) storage class 30 days after creation or archive objects to the GLACIER storage class one year after creation.

**Expiration actions** – In which you specify when the objects expire. Then Amazon S3 deletes the expired objects on your behalf.

**Use Server-Side Encryption** – You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.

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

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

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

**Use Client-Side Encryption** – You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

Use Client-Side Encryption with AWS KMS–Managed Customer Master Key (CMK)

Use Client-Side Encryption Using a Client-Side Master Key

A tech startup is launching an on-demand food delivery platform using Amazon ECS cluster with an AWS Fargate serverless compute engine and Amazon Aurora. It is expected that the database read queries will significantly increase in the coming weeks ahead. A Solutions Architect recently launched two Read Replicas to the database cluster to improve the platform's scalability.

Which of the following is the MOST suitable configuration that the Architect should implement to load balance all of the incoming read requests equally to the two Read Replicas?

ANS: A reader endpoint for an Aurora DB cluster provides load-balancing support for read-only connections to the DB cluster. Use the reader endpoint for read operations, such as queries.

INCORRECT: **Enable Amazon Aurora Parallel Query**is incorrect because this feature simply enables Amazon Aurora to push down and distribute the computational load of a single query across thousands of CPUs in Aurora's storage layer. Take note that it does not load balance all of the incoming read requests equally to the two Read Replicas. With Parallel Query, query processing is pushed down to the Aurora storage layer. The query gains a large amount of computing power, and it needs to transfer far less data over the network. In the meantime, the Aurora database instance can continue serving transactions with much less interruption. This way, you can run transactional and analytical workloads alongside each other in the same Aurora database, while maintaining high performance.

Here is a list of important information about EBS Volumes:

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

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

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

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

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

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

- EBS Volumes offer 99.999% SLA.

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

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

ANS: **Alias with a type "AAAA" record set** and **Alias with a type "A" record set.**

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

INCORRECT: **Non-Alias with a type "A" record set** is incorrect because you only use Non-Alias with a type “A” record set for IP addresses.

**Alias with a type "CNAME" record set** is incorrect because you can't create a CNAME record at the zone apex. For example, if you register the DNS name tutorialsdojo.com, the zone apex is tutorialsdojo.com.

**Alias with a type of “MX” record set** is incorrect because an MX record is primarily used for mail servers. It includes a priority number and a domain name, for example: 10 mailserver.tutorialsdojo.com.