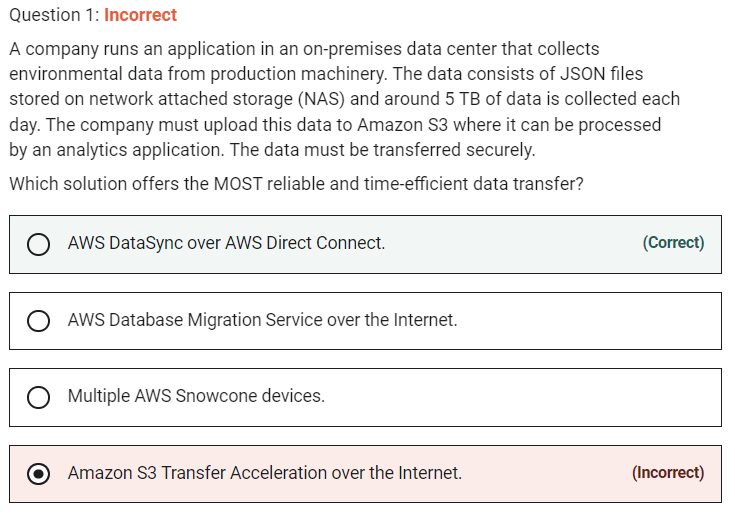
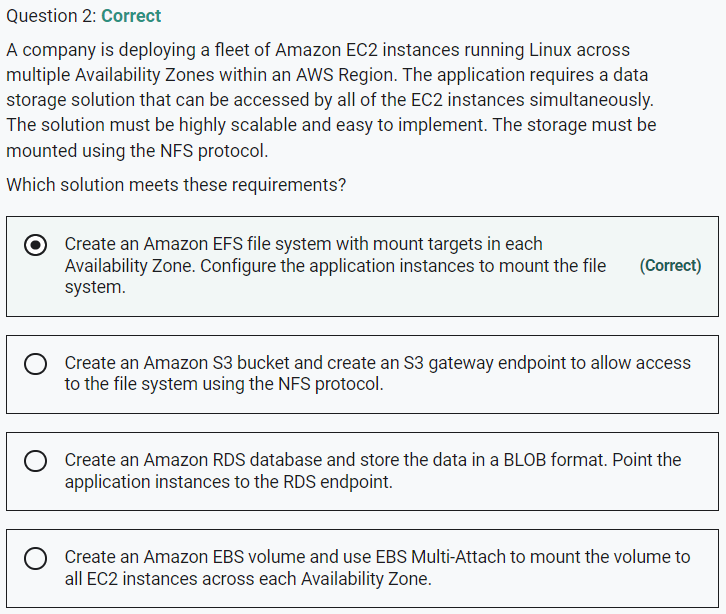
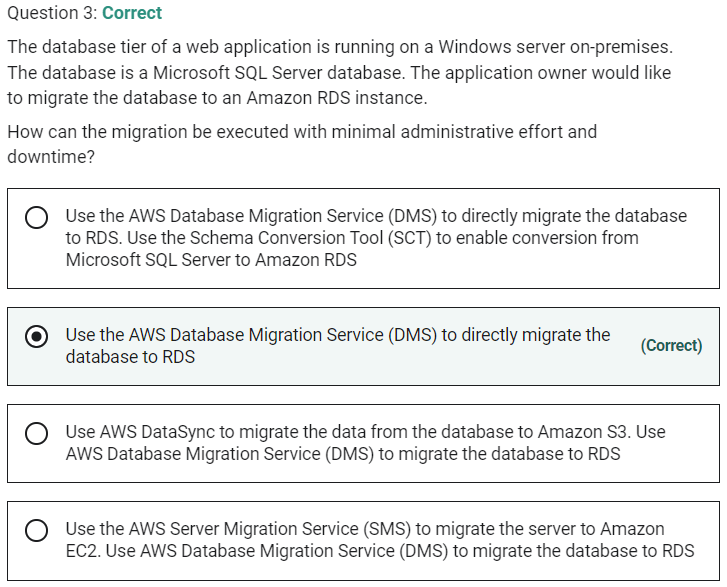
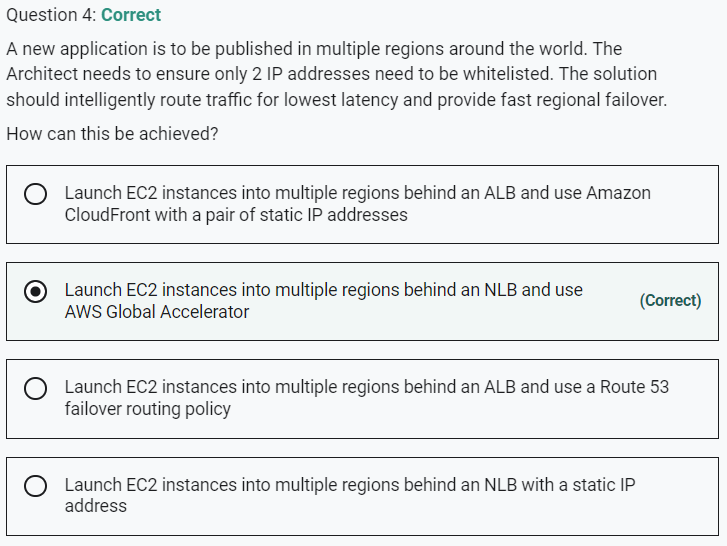
SAA-CO2

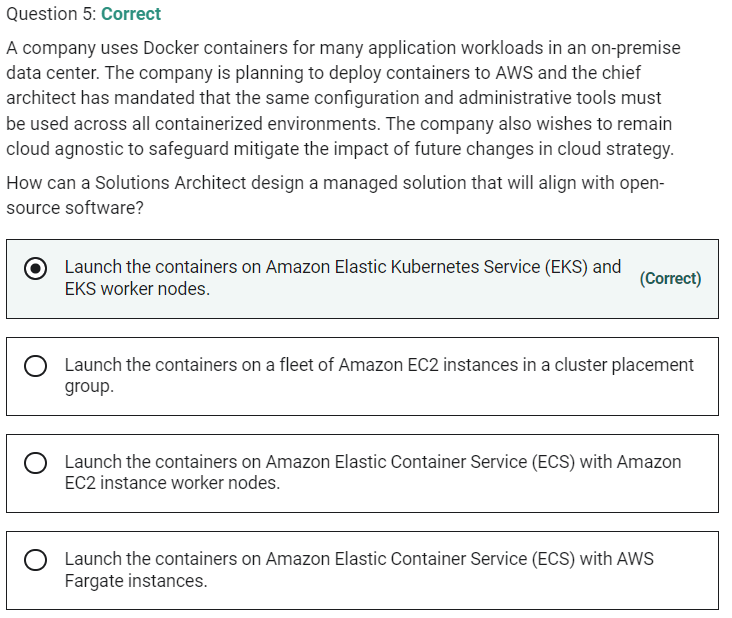
Practice Test 7

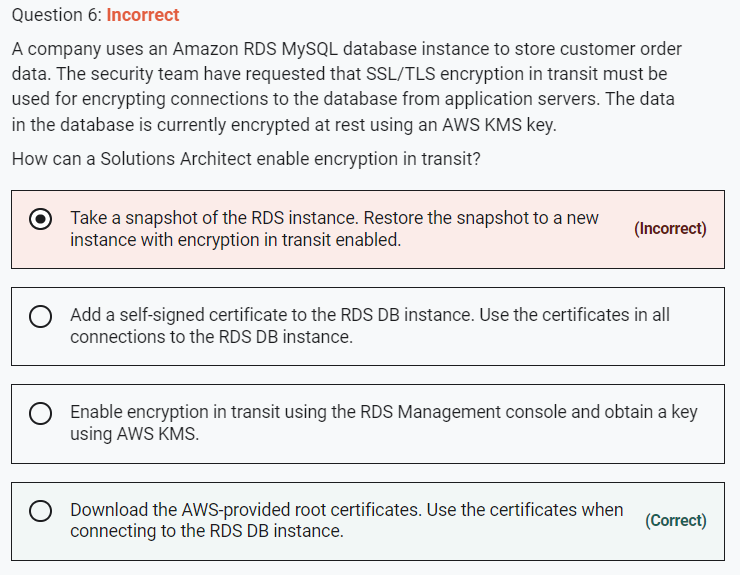




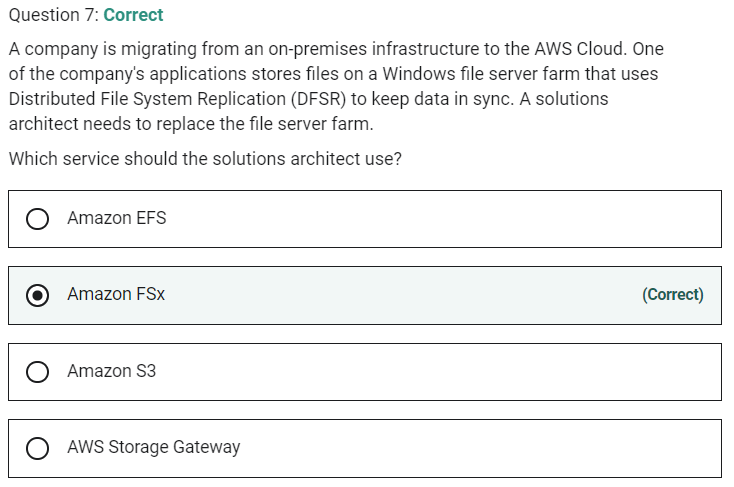


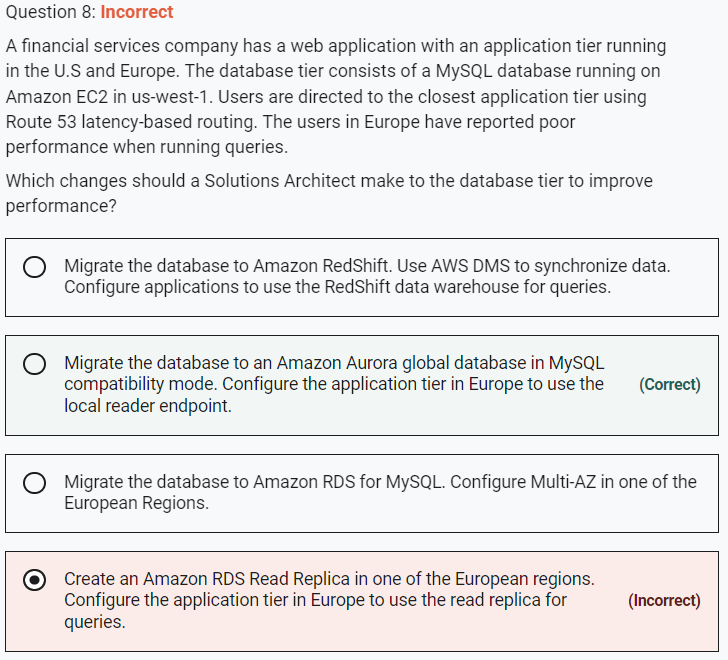






 "Enable encryption in transit using the RDS Management console and obtain a key using AWS KMS" is incorrect. You cannot enable/disable encryption in transit using the RDS management console or use a KMS key.

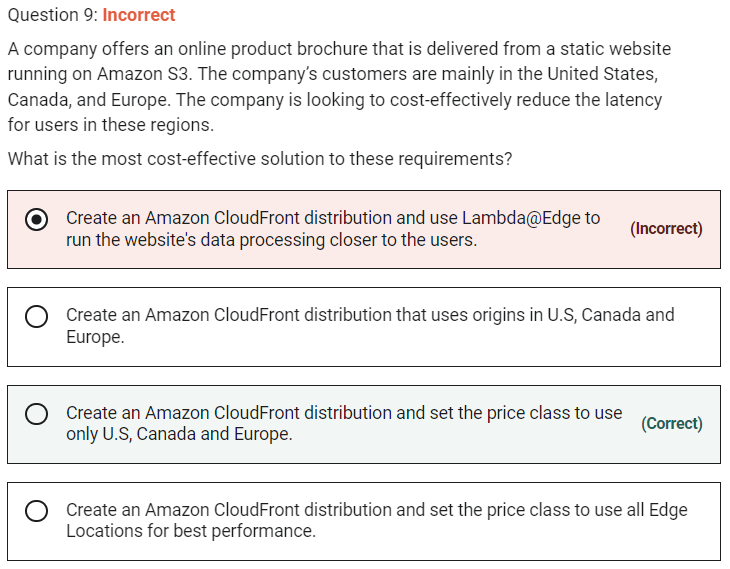




**INCORRECT:** "Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in one of the European Regions" is incorrect. You cannot configure a multi-AZ DB instance to run in another Region, it must be in the same Region but in a different Availability Zone.

**INCORRECT:** "Migrate the database to Amazon RedShift. Use AWS DMS to synchronize data. Configure applications to use the RedShift data warehouse for queries" is incorrect. RedShift is a data warehouse and used for running analytics queries on data that is exported from transactional database systems. It should not be used to reduce latency for users of a database, and is not a live copy of the data.

**INCORRECT:** "Create an Amazon RDS Read Replica in one of the European regions. Configure the application tier in Europe to use the read replica for queries" is incorrect. You cannot create an RDS Read Replica of a database that is running on Amazon EC2. You can only create read replicas of databases running on Amazon RDS.



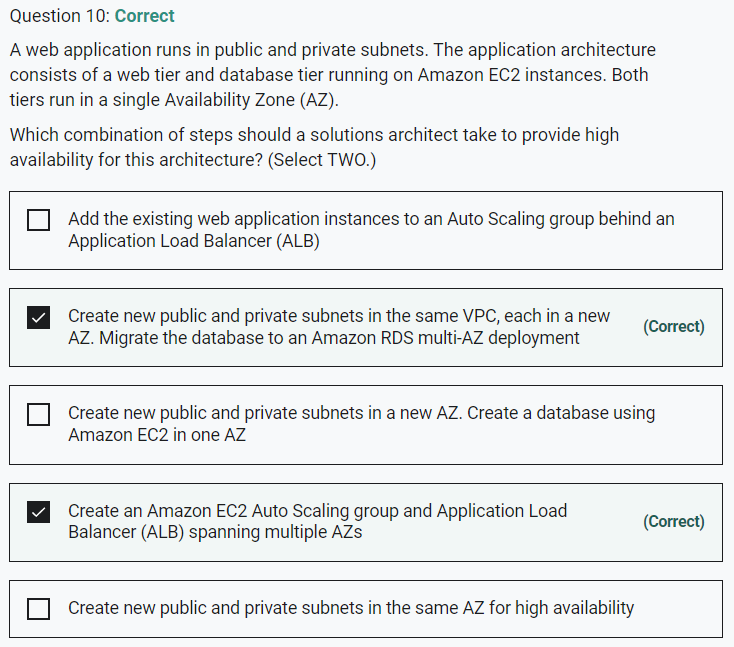
With Amazon CloudFront you can set the price class to determine where in the world the content will be cached

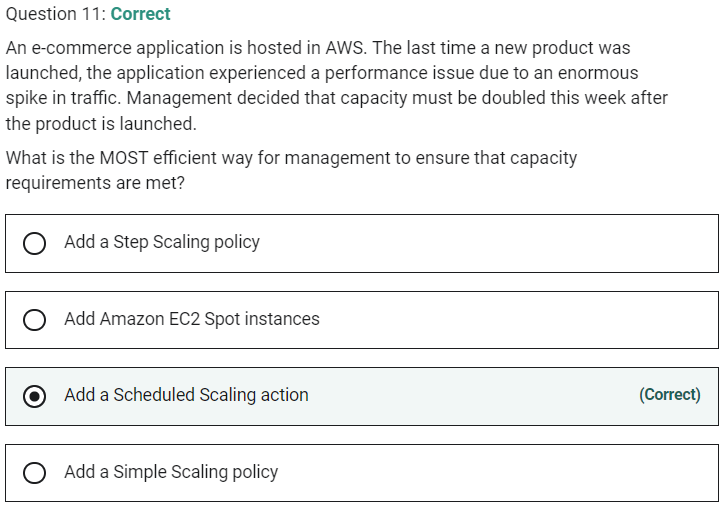
**CORRECT:**"Create an Amazon CloudFront distribution and set the price class to use only U.S, Canada and Europe." is the correct answer.

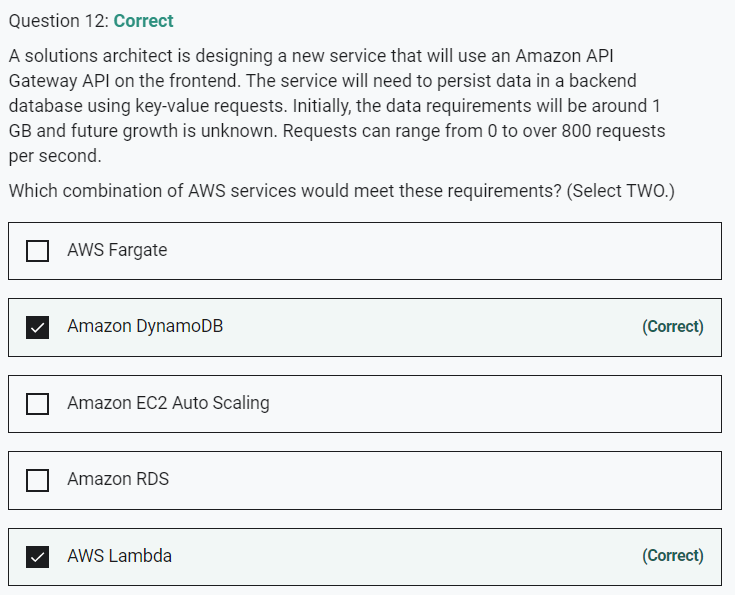
**INCORRECT:** "Create an Amazon CloudFront distribution and set the price class to use all Edge Locations for best performance" is incorrect. This will be more expensive as it will cache content in Edge Locations all over the world.

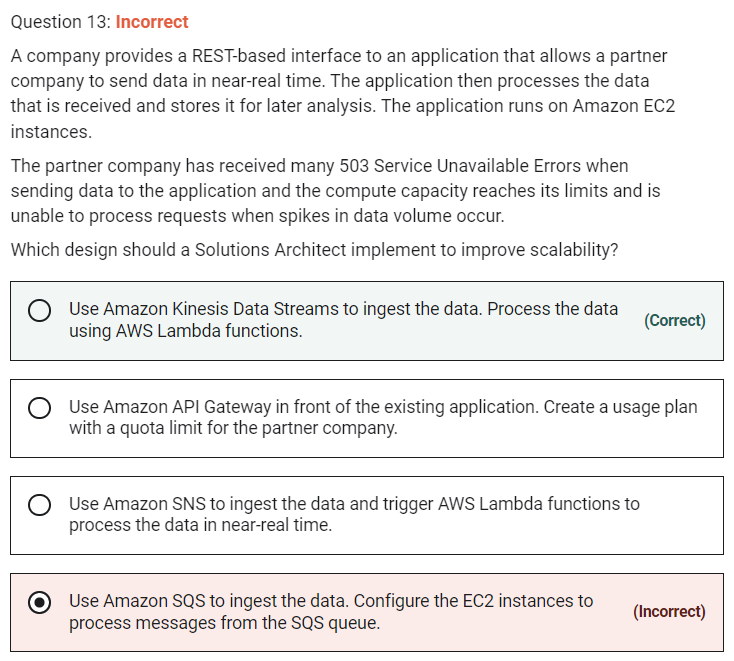
**INCORRECT:** "Create an Amazon CloudFront distribution that uses origins in U.S, Canada and Europe" is incorrect. The origin can be in one place, there’s no need to add origins in different Regions. The price class should be used to limit the caching of the content to reduce cost.

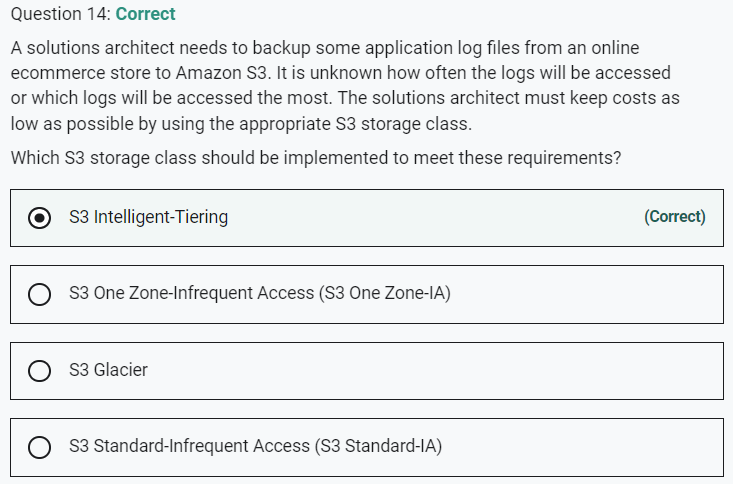
**INCORRECT:** "Create an Amazon CloudFront distribution and use Lambda@Edge to run the website's data processing closer to the users" is incorrect. Lambda@Edge will not assist in this situation as there is no data processing required, the content from the static website must simply be cached at an edge location.

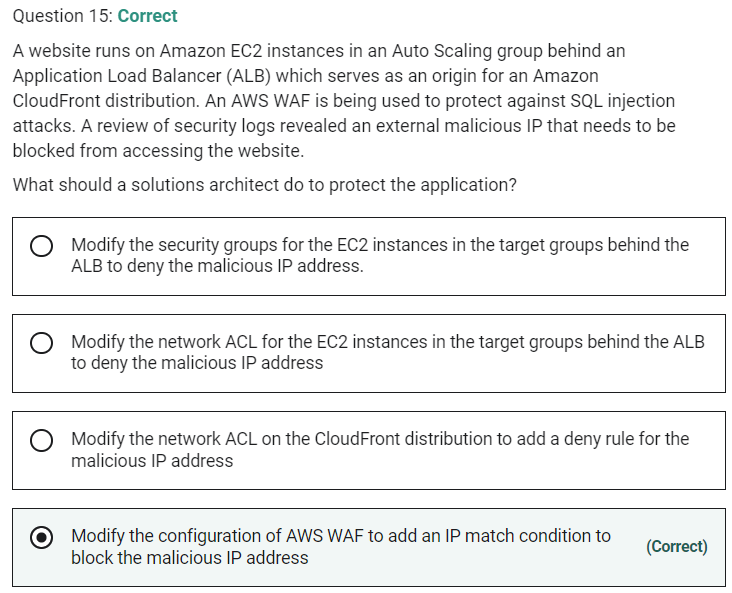


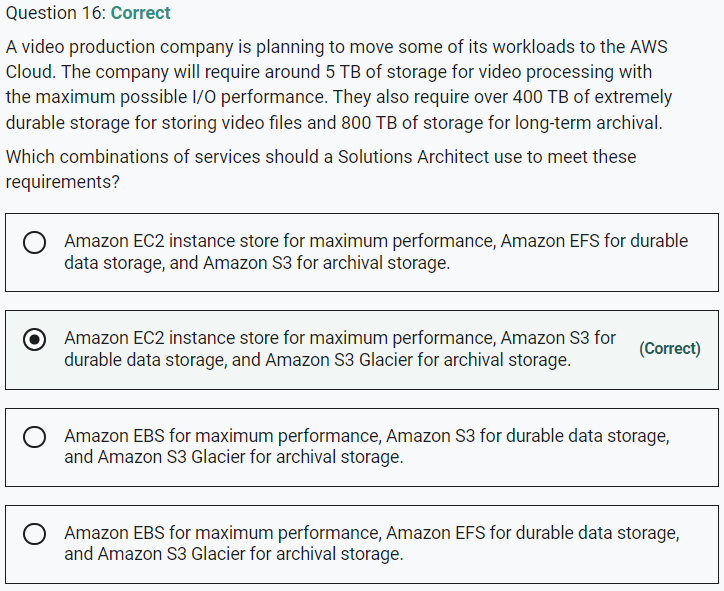


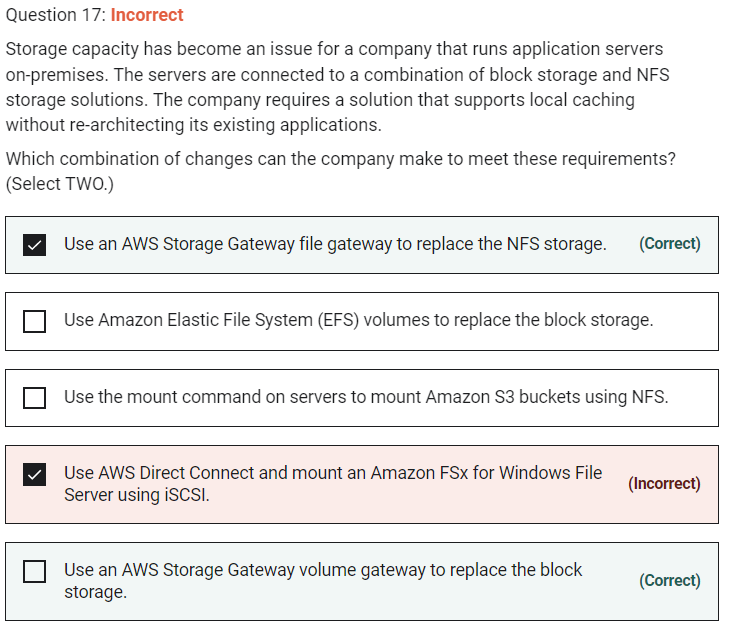


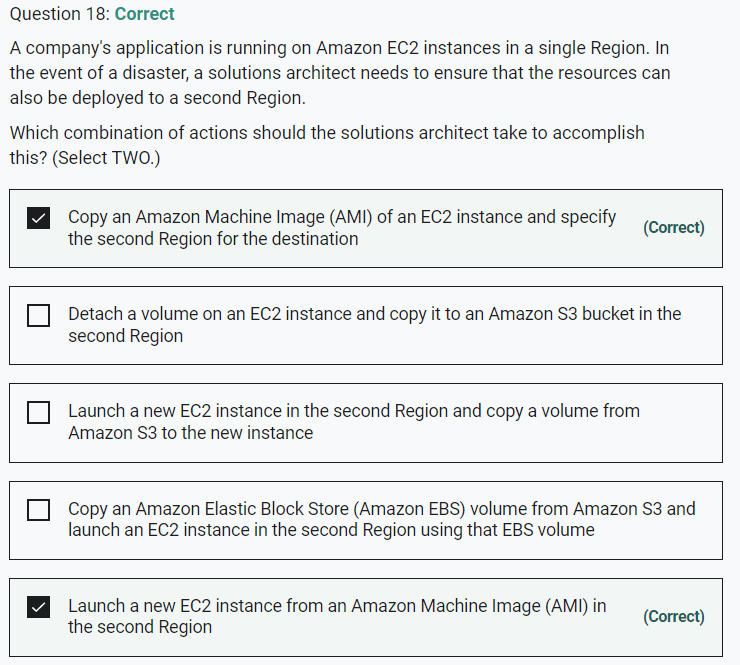


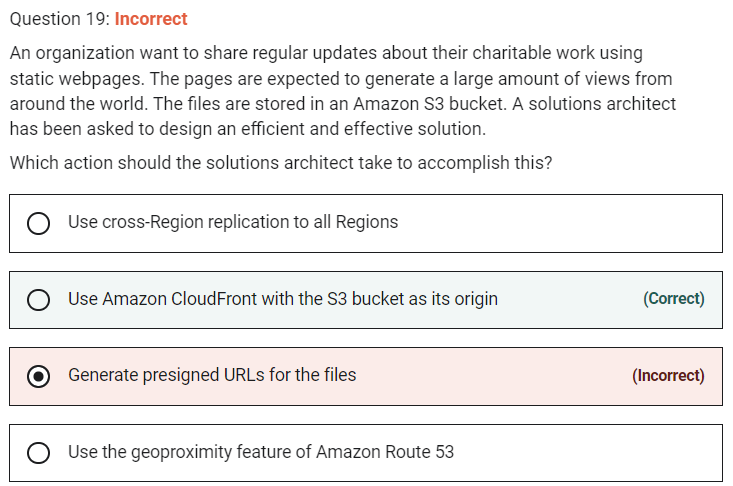


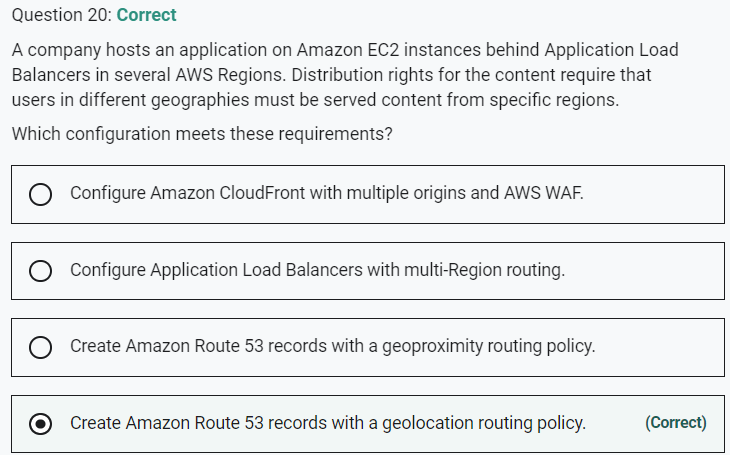


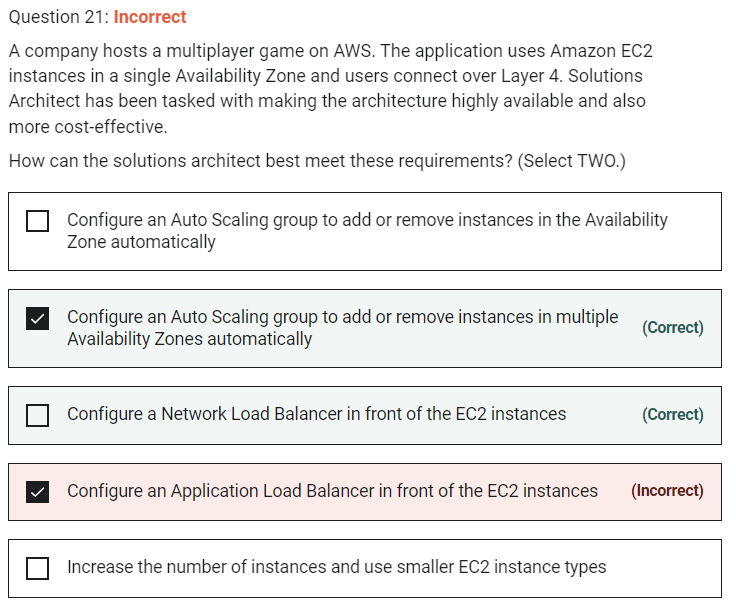


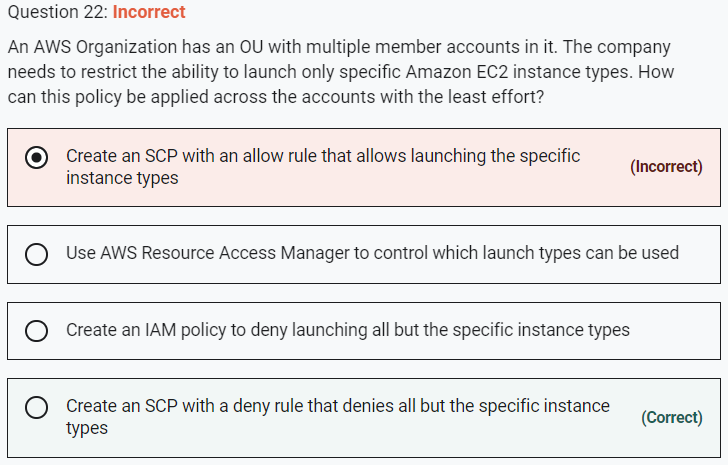


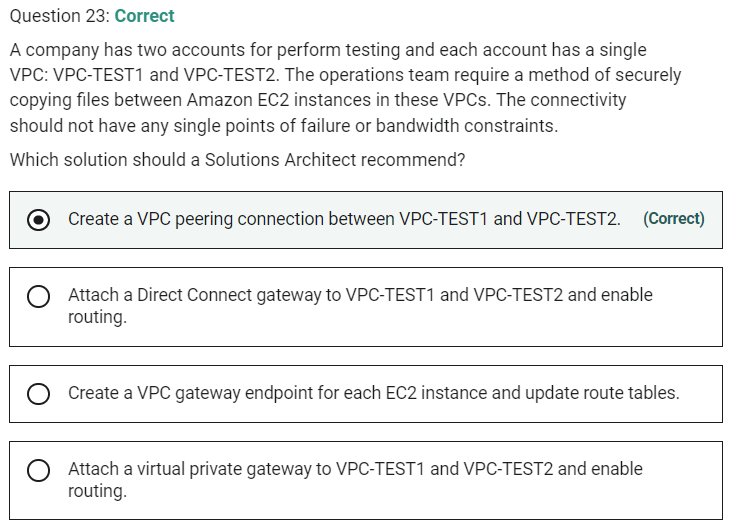


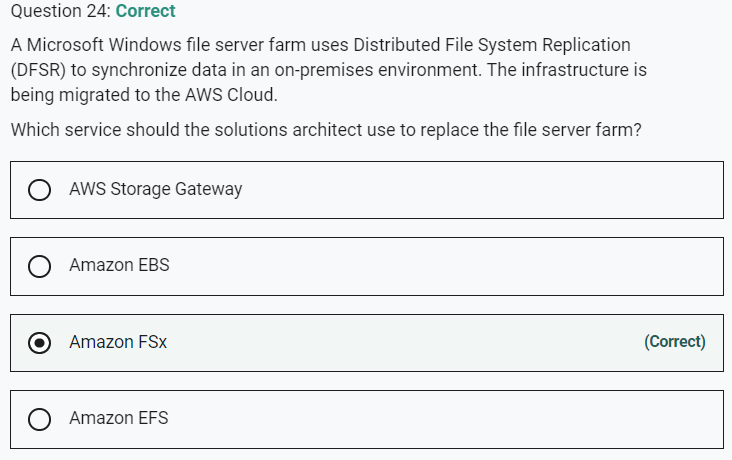


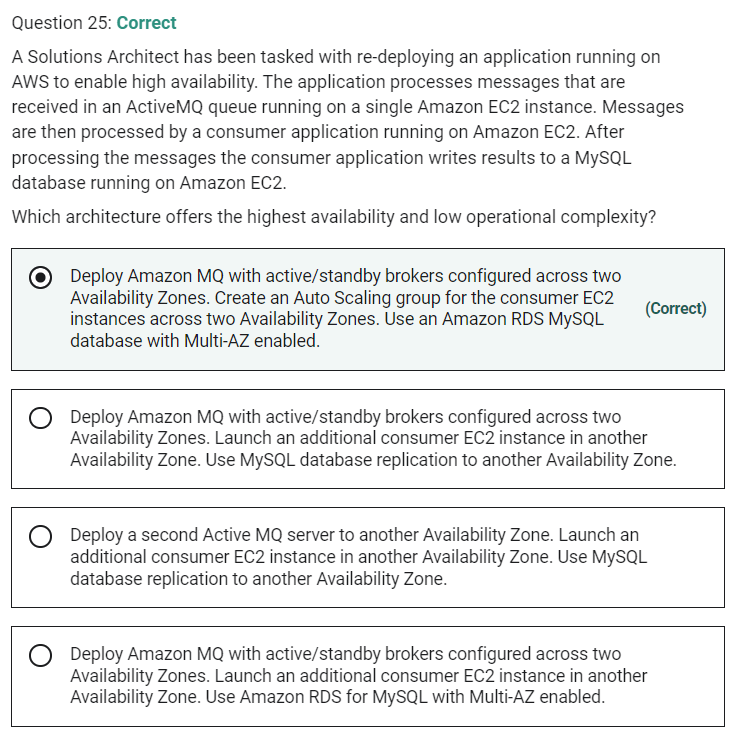


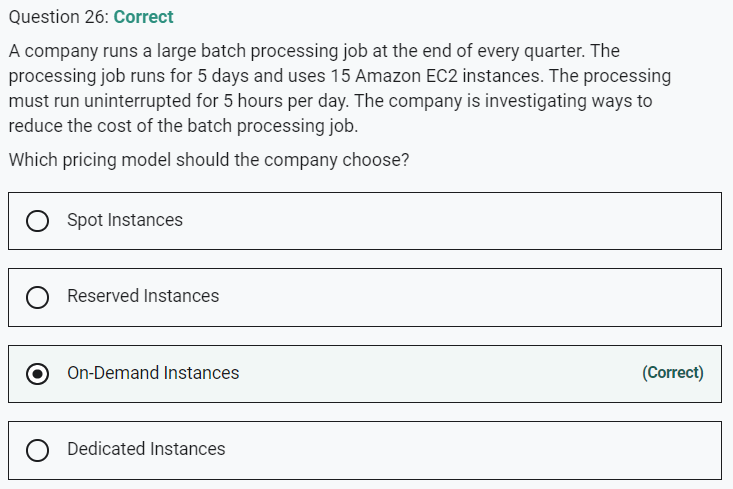








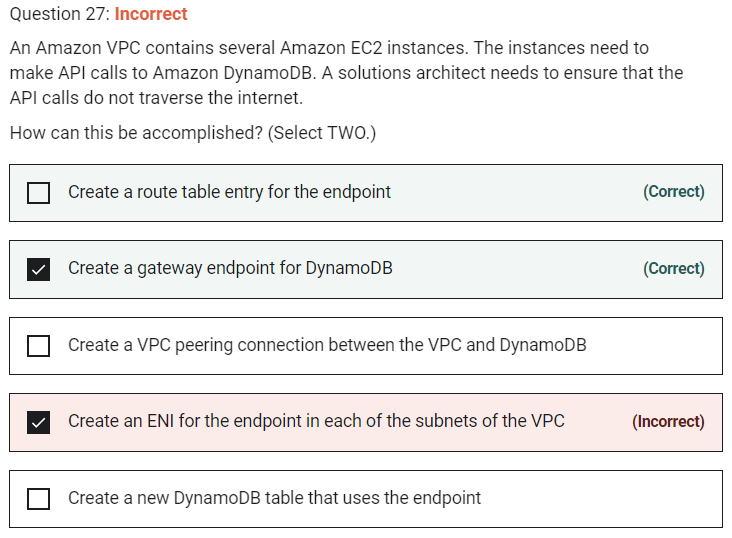


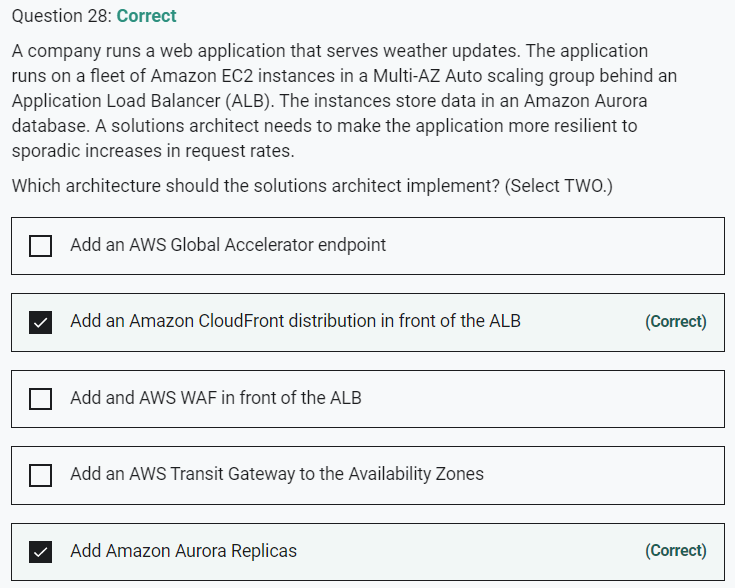


Each EC2 instance runs for 5 hours a day for 5 days per quarter or 20 days per year. This is time duration is insufficient to warrant reserved instances as these require a commitment of a minimum of 1 year and the discounts would not outweigh the costs of having the reservations unused for a large percentage of time. In this case, there are no options presented that can reduce the cost and therefore on-demand instances should be used.

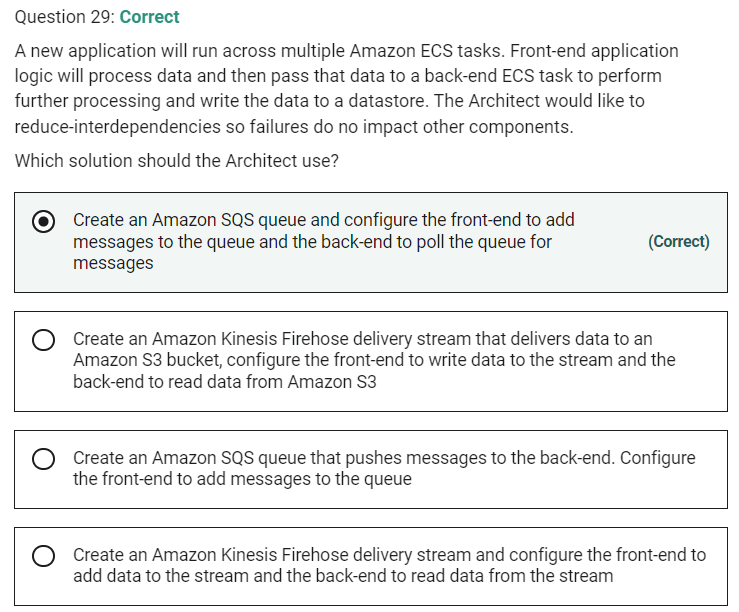
**CORRECT:**"On-Demand Instances" is the correct answer.

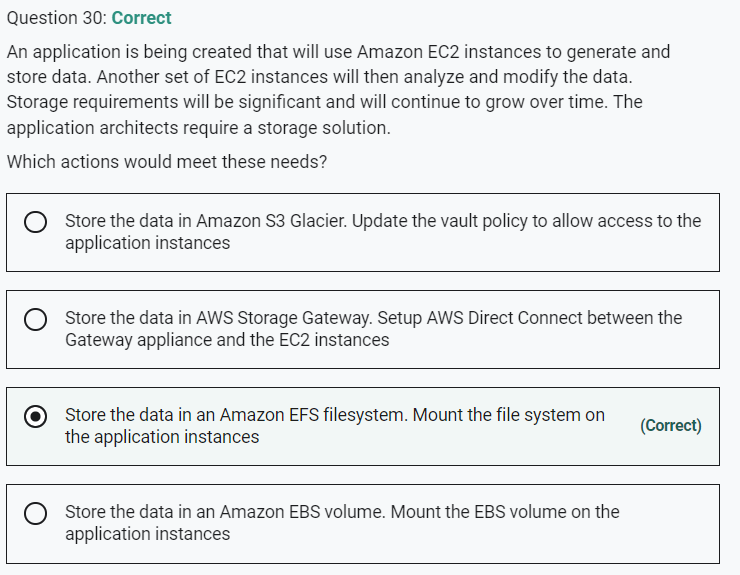
**INCORRECT:** "Reserved Instances" is incorrect. Reserved instances are good for continuously running workloads that run for a period of 1 or 3 years.

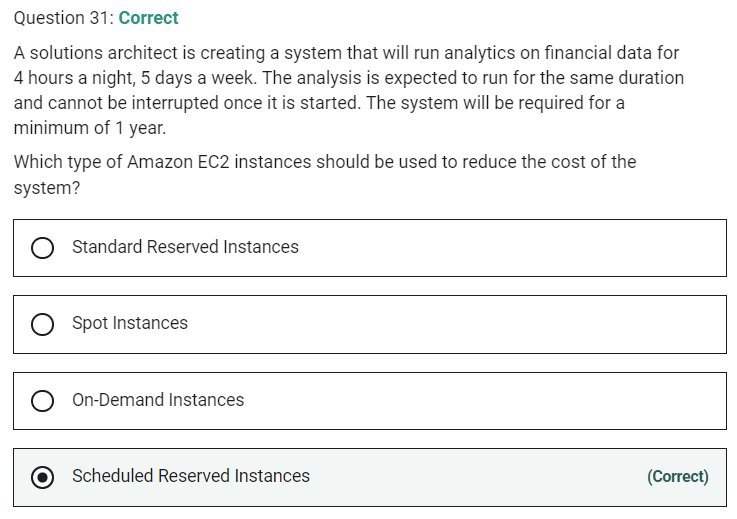


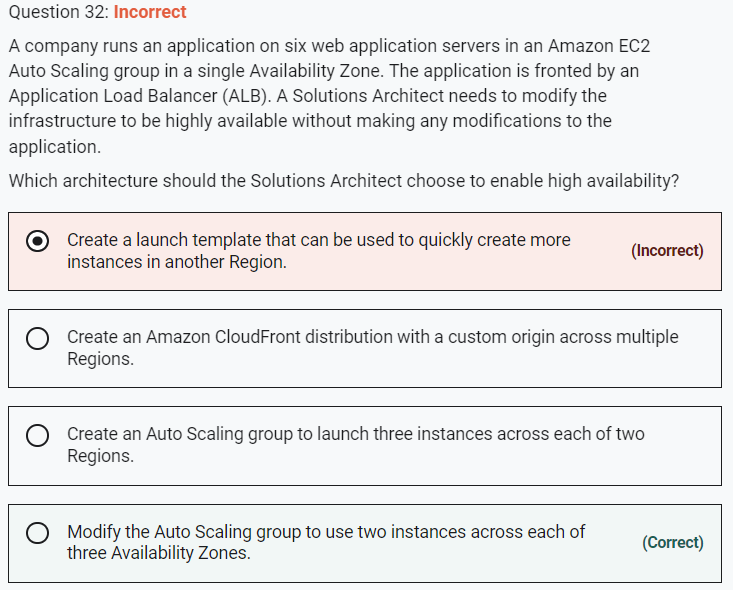


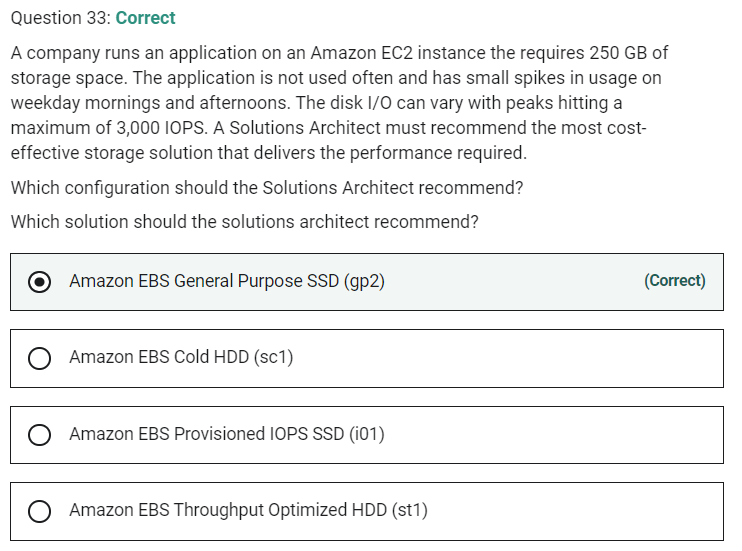
"Add an AWS Global Accelerator endpoint" is incorrect as this service is used for directing users to different instances of the application in different regions based on latency.

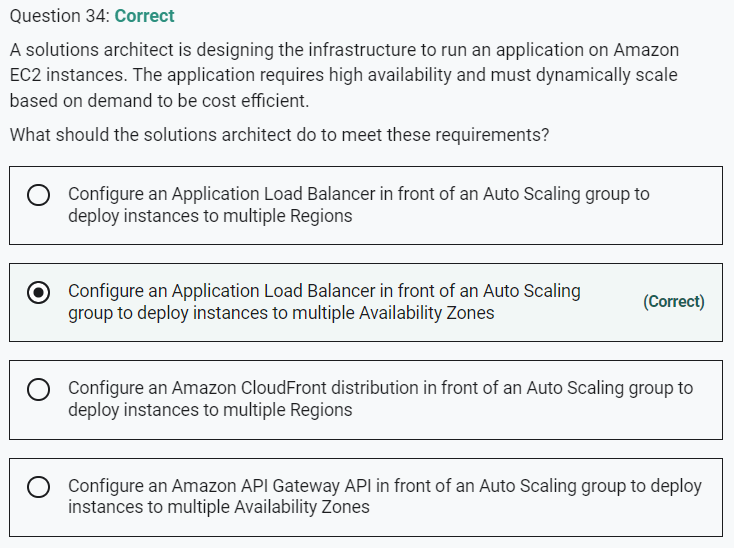












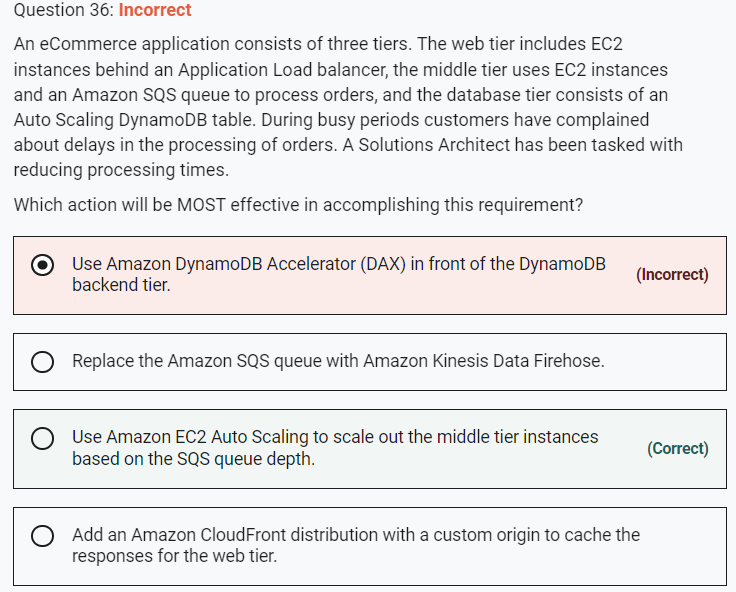


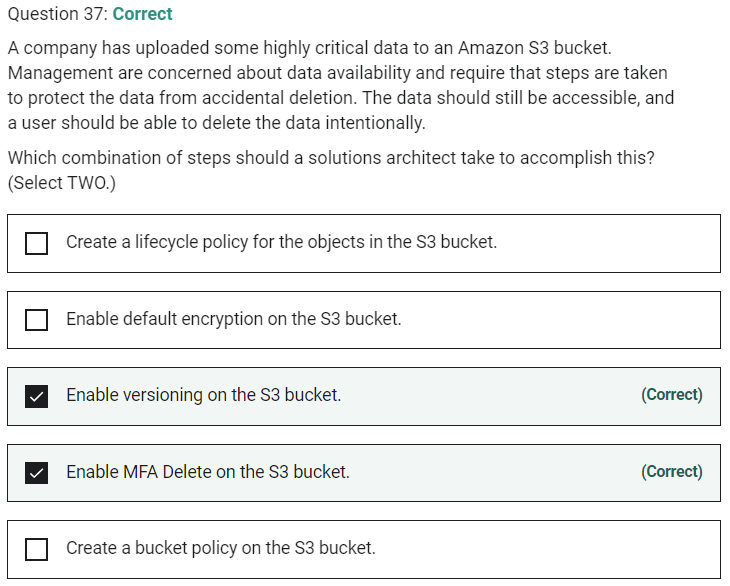
When a user requests your content, CloudFront typically serves the requested content regardless of where the user is located. If you need to prevent users in specific countries from accessing your content, you can use the CloudFront geo restriction feature to do one of the following:

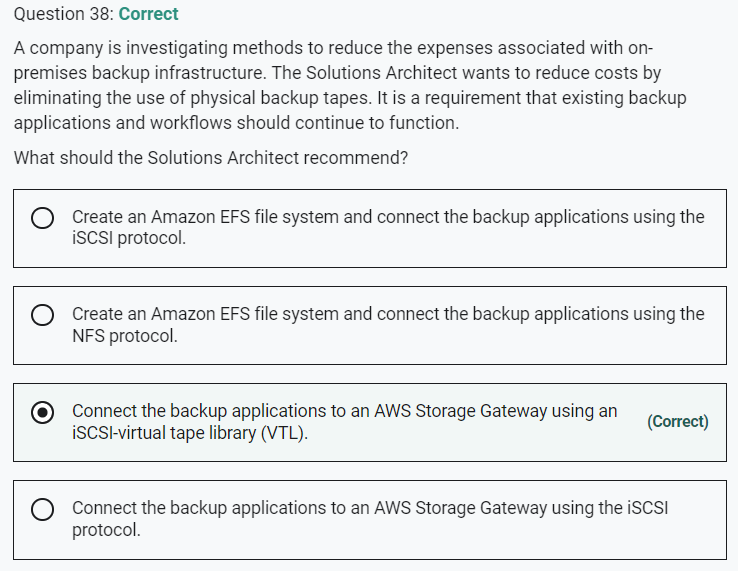
Allow your users to access your content only if they're in one of the countries on a whitelist of approved countries.

Prevent your users from accessing your content if they're in one of the countries on a blacklist of banned countries.

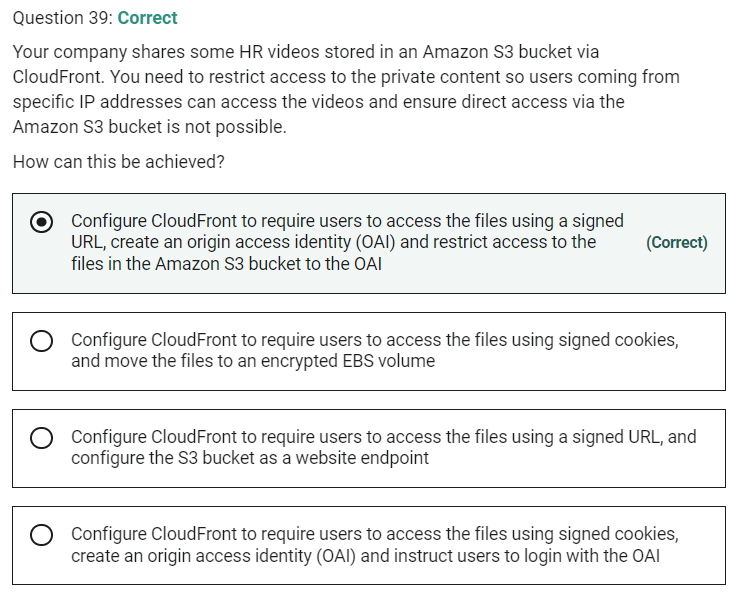
For example, if a request comes from a country where, for copyright reasons, you are not authorized to distribute your content, you can use CloudFront geo restriction to block the request.

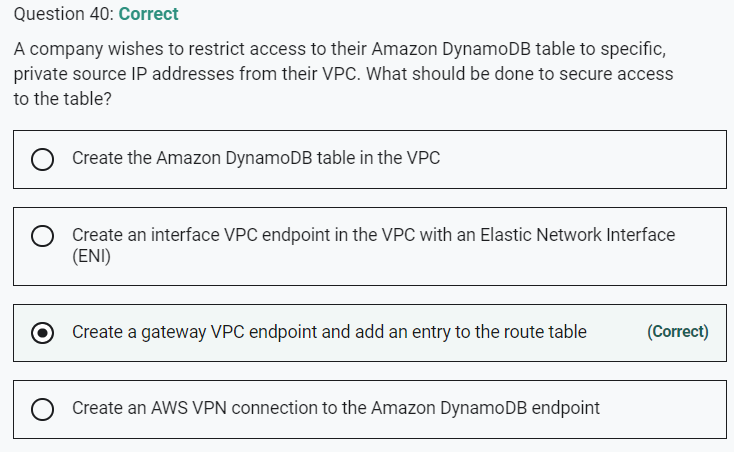


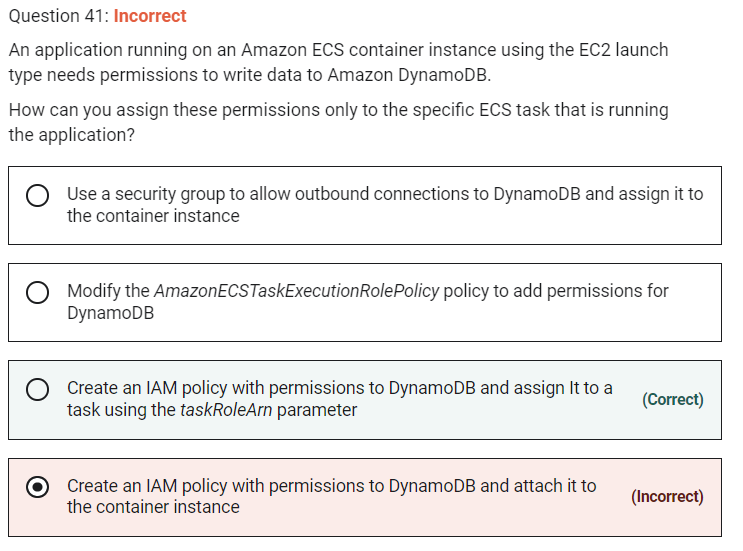


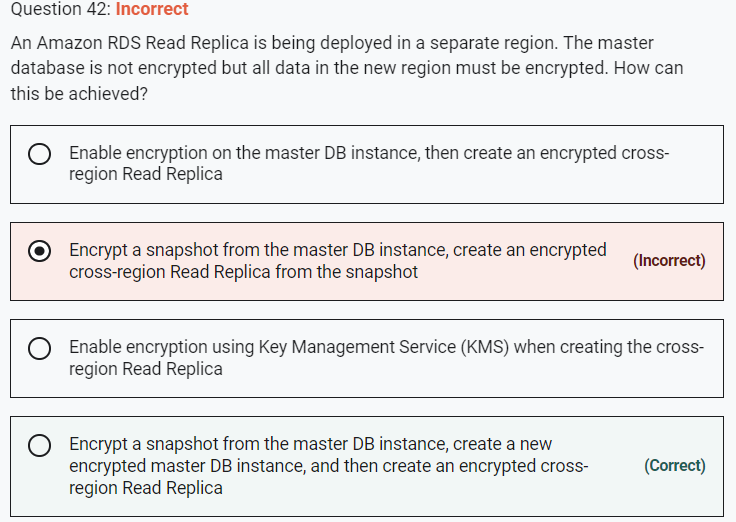


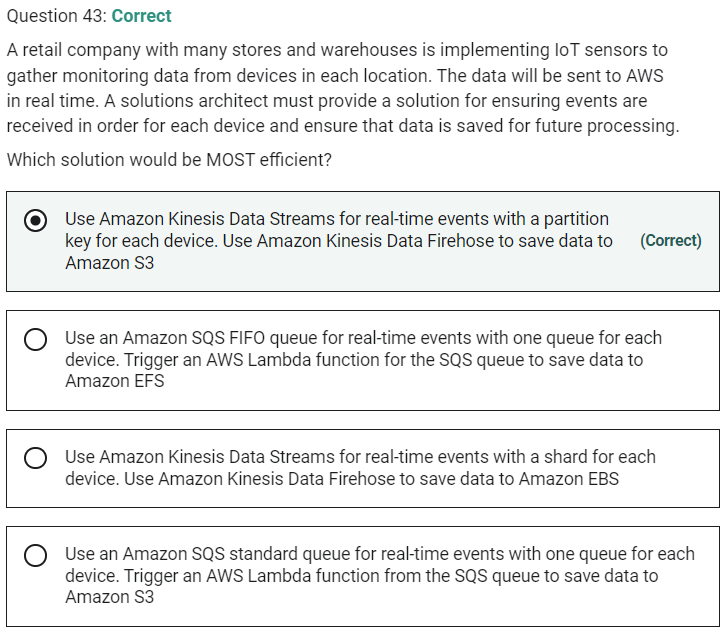
The AWS Storage Gateway Tape Gateway enables you to replace using physical tapes on premises with virtual tapes in AWS without changing existing backup workflows.

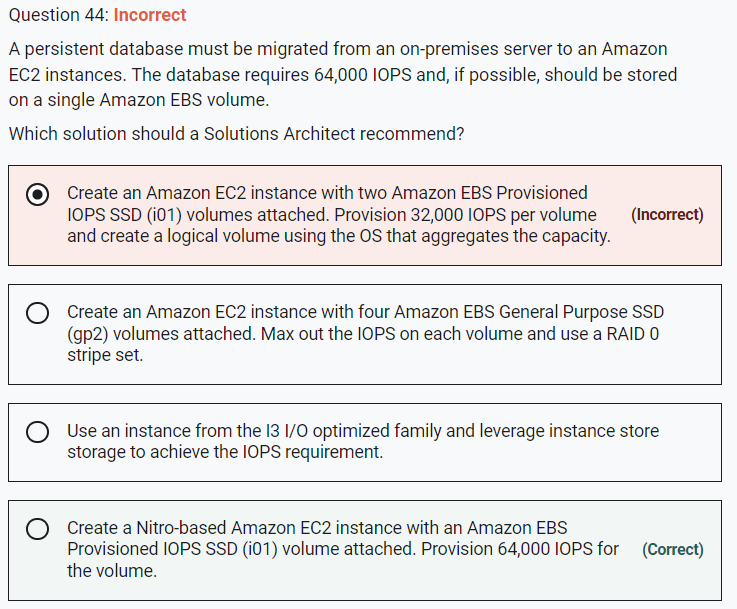


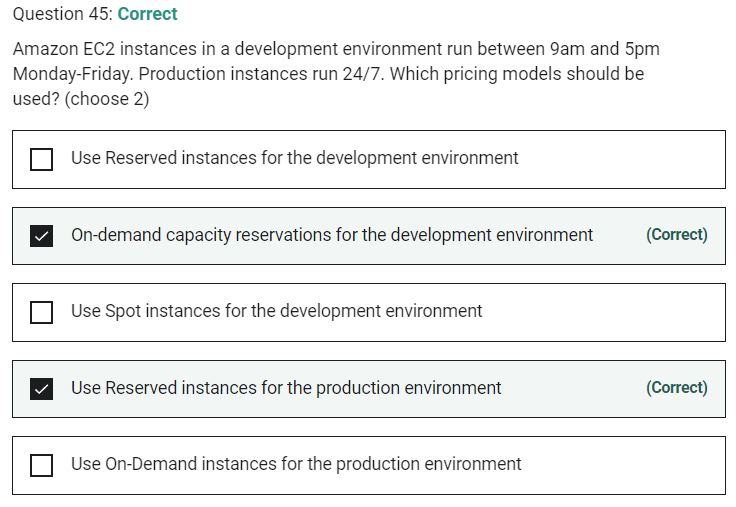


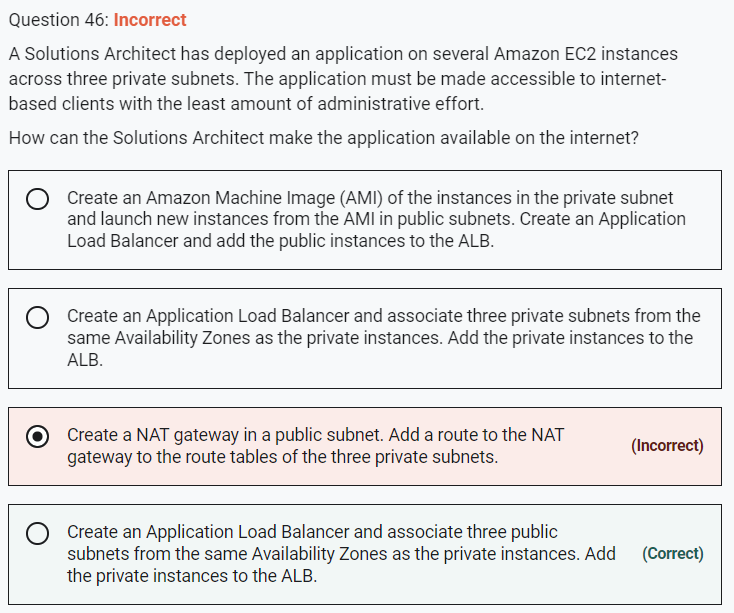




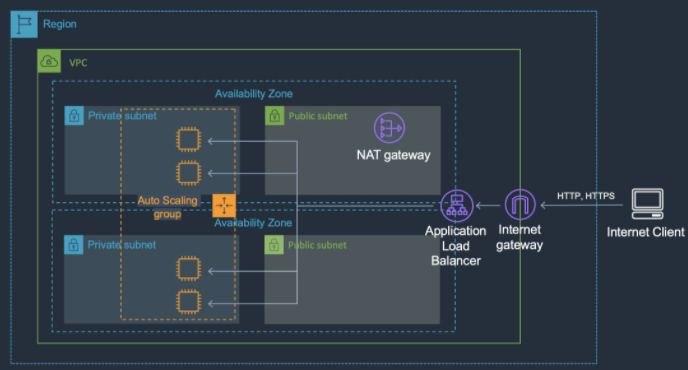




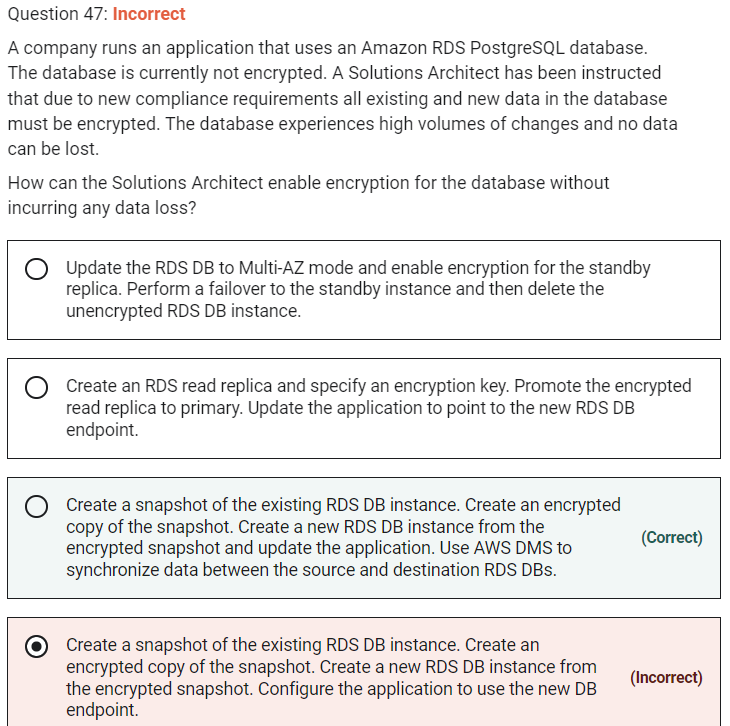




To make the application instances accessible on the internet the Solutions Architect needs to place them behind an internet-facing Elastic Load Balancer. The way you add instances in private subnets to a public facing ELB is to add public subnets in the same AZs as the private subnets to the ELB. You can then add the instances and to the ELB and they will become targets for load balancing.

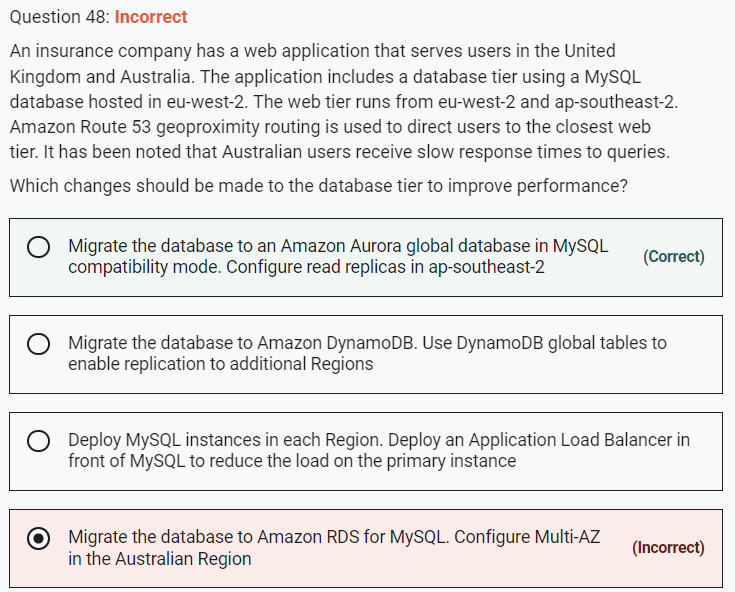


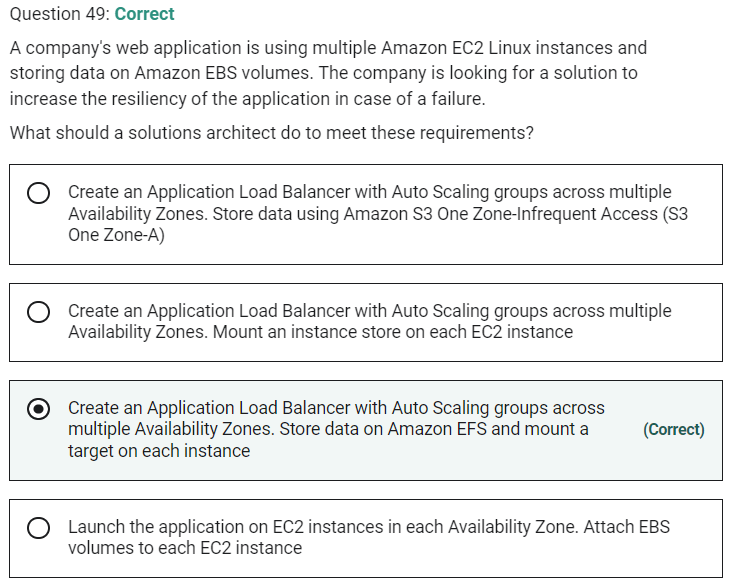
**INCORRECT:** "Create a NAT gateway in a public subnet. Add a route to the NAT gateway to the route tables of the three private subnets" is incorrect. A NAT gateway is used for outbound traffic not inbound traffic and cannot make the application available to internet-based clients.

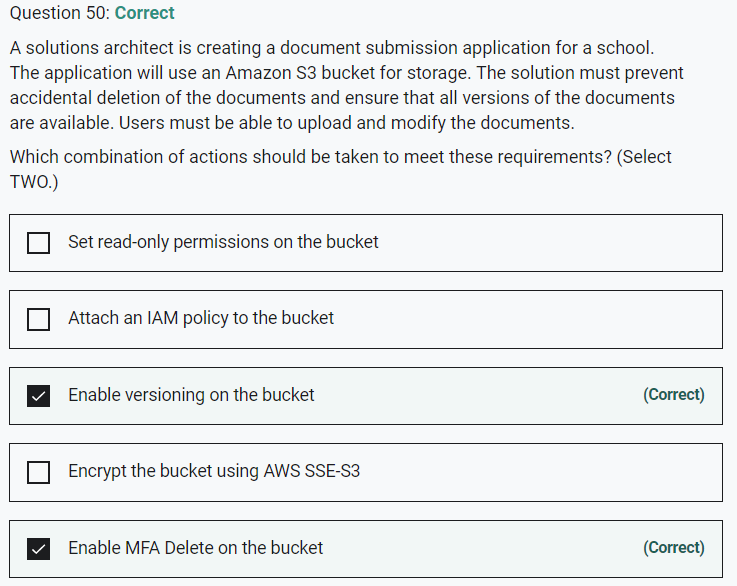


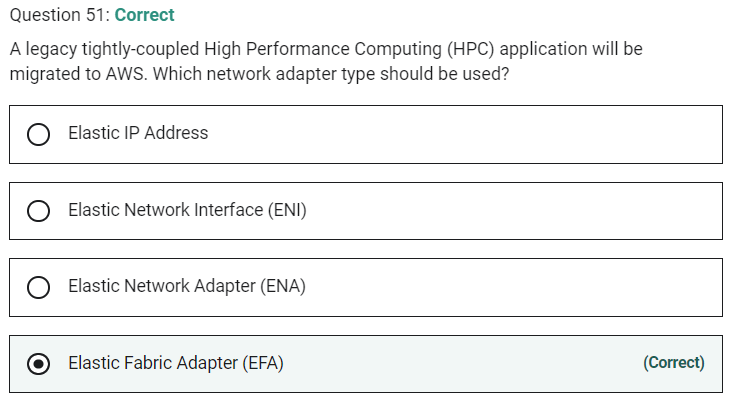
You cannot change the encryption status of an existing RDS DB instance. Encryption must be specified when creating the RDS DB instance. The best way to encrypt an existing database is to take a snapshot, encrypt a copy of the snapshot and restore the snapshot to a new RDS DB instance. This results in an encrypted database that is a new instance. Applications must be updated to use the new RDS DB endpoint.

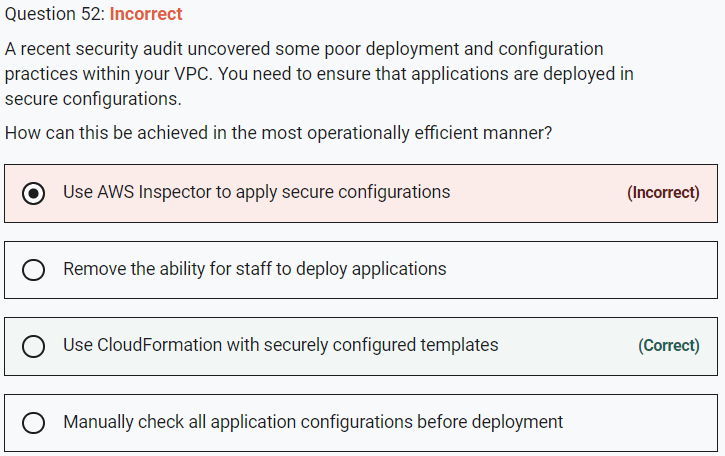
In this scenario as there is a high rate of change, the databases will be out of sync by the time the new copy is created and is functional. The best way to capture the changes between the source (unencrypted) and destination (encrypted) DB is to use AWS Database Migration Service (DMS) to synchronize the data.





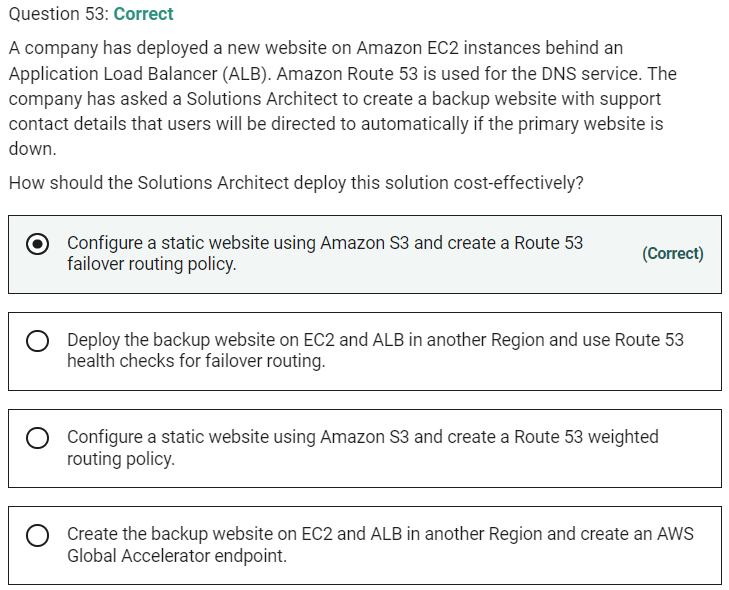


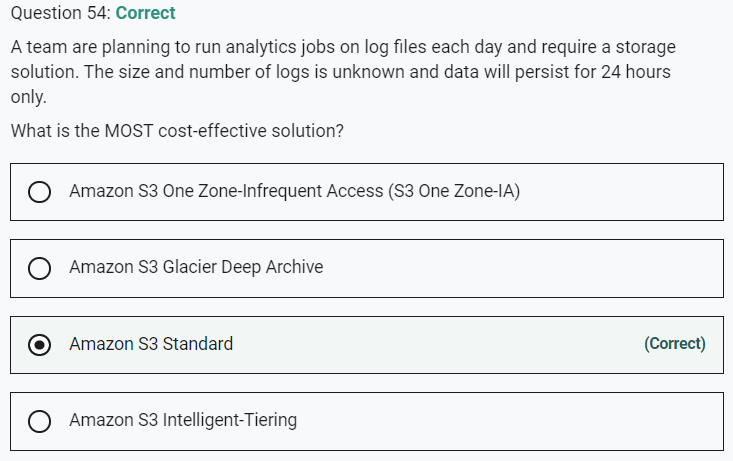




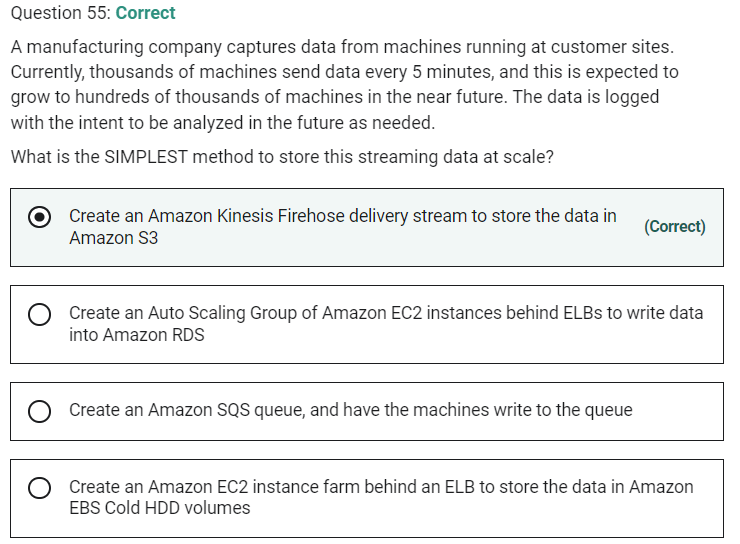
CloudFormation helps users to deploy resources in a consistent and orderly way. By ensuring the CloudFormation templates are created and administered with the right security configurations for your resources, you can then repeatedly deploy resources with secure settings and reduce the risk of human error.

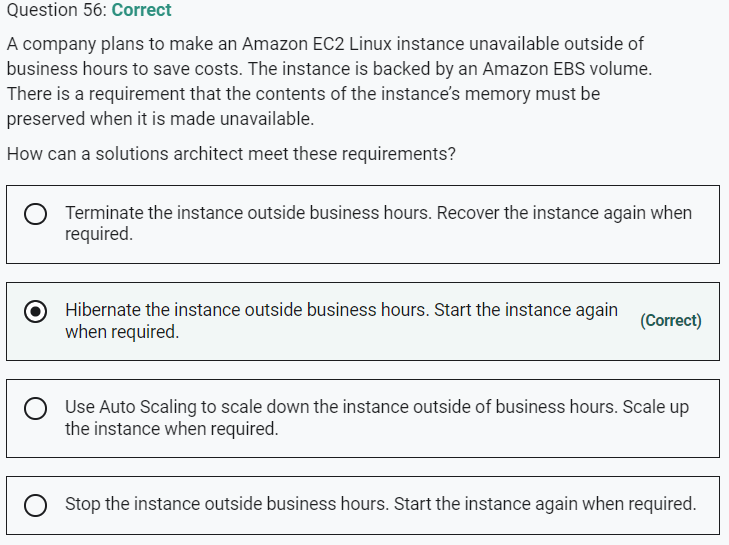
**INCORRECT:** "Use AWS Inspector to apply secure configurations" is incorrect. Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications **deployed** on AWS. It is not used to secure the actual deployment of resources, only to assess the deployed state of the resources.

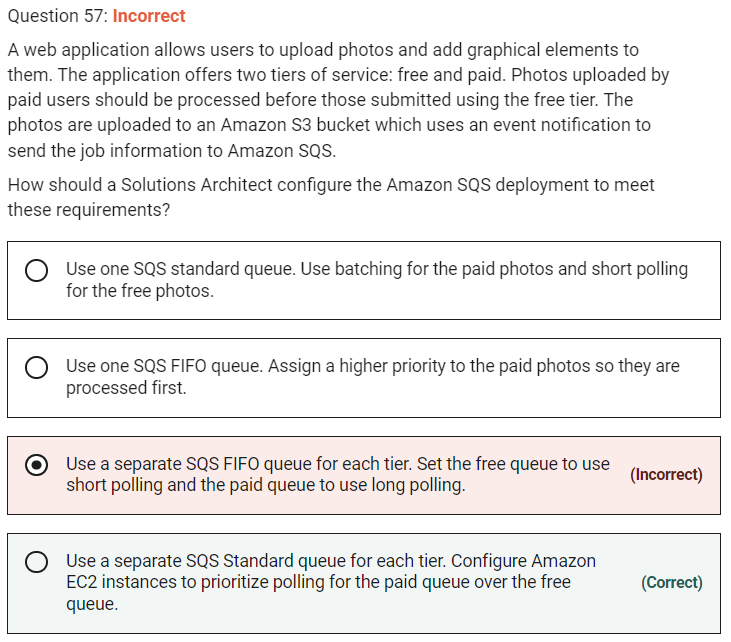


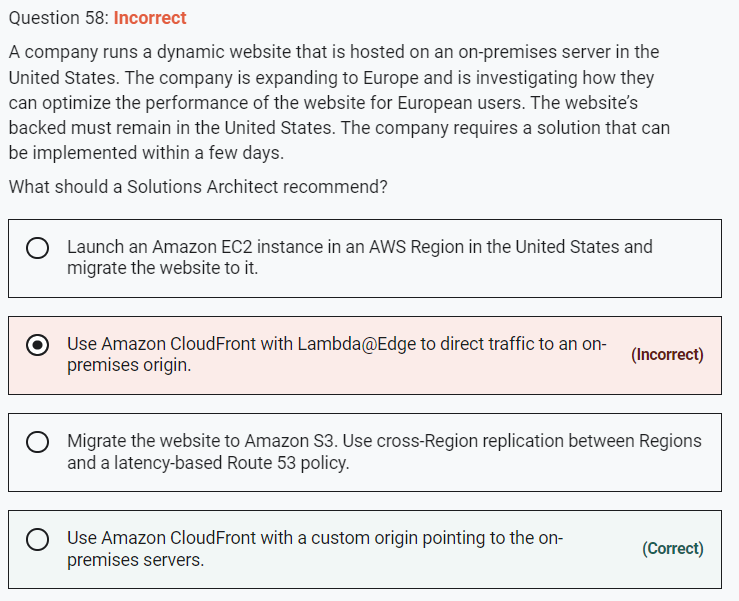


S3 standard is the best choice in this scenario for a short term storage solution. In this case the size and number of logs is unknown and it would be difficult to fully assess the access patterns at this stage. Therefore, using S3 standard is best as it is cost-effective, provides immediate access, and there are no retrieval fees or minimum capacity charge per object.









A custom origin can point to an on-premises server and CloudFront is able to cache content for dynamic websites. CloudFront can provide performance optimizations for custom origins even if they are running on on-premises servers. These include persistent TCP connections to the origin, SSL enhancements such as Session tickets and OCSP stapling.

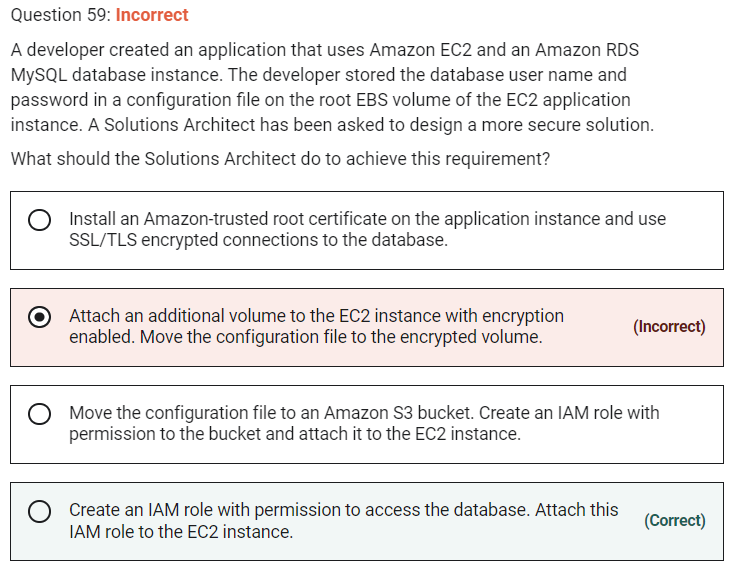
Additionally, connections are routed from the nearest Edge Location to the user across the AWS global network. If the on-premises server is connected via a Direct Connect (DX) link this can further improve performance.

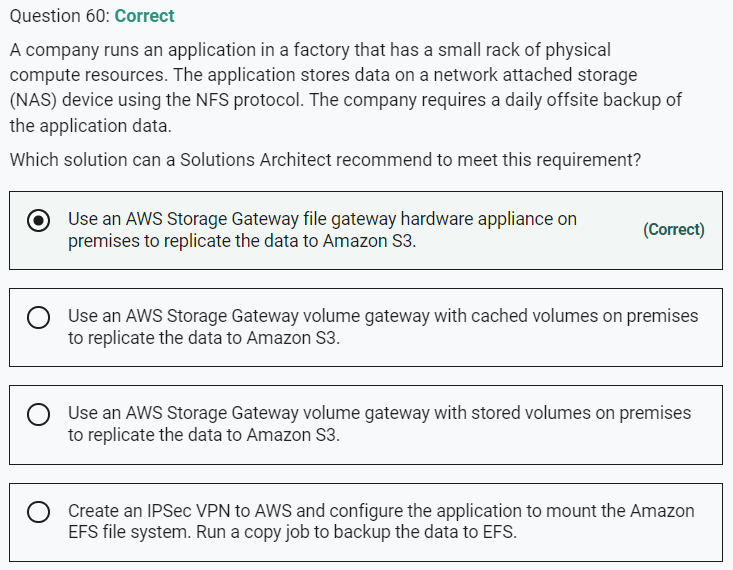
**CORRECT:**"Use Amazon CloudFront with a custom origin pointing to the on-premises servers" is the correct answer.

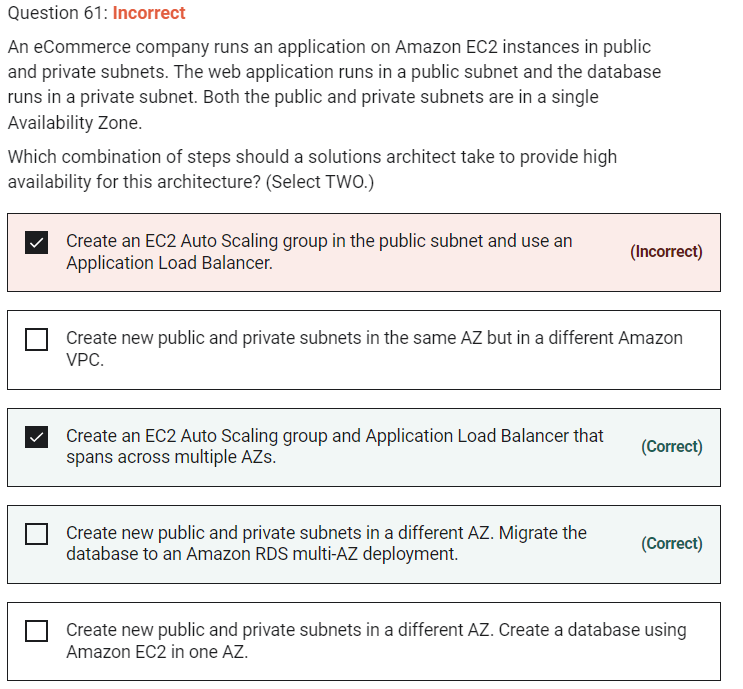
**INCORRECT:** "Use Amazon CloudFront with Lambda@Edge to direct traffic to an on-premises origin" is incorrect. Lambda@Edge is not used to direct traffic to on-premises origins.

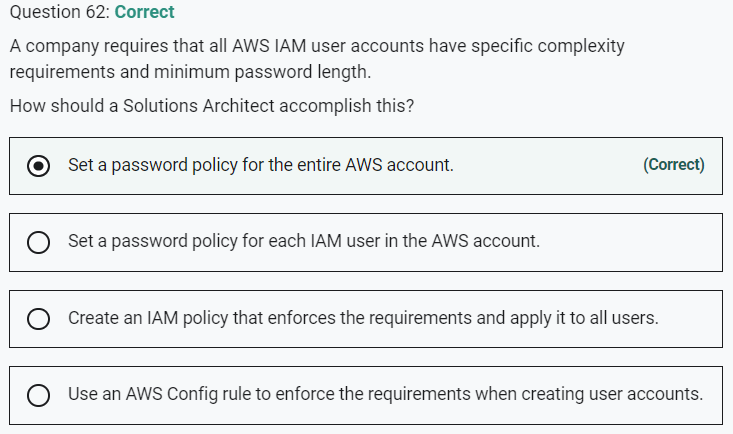
**INCORRECT:** "Launch an Amazon EC2 instance in an AWS Region in the United States and migrate the website to it" is incorrect. This would not necessarily improve performance for European users.

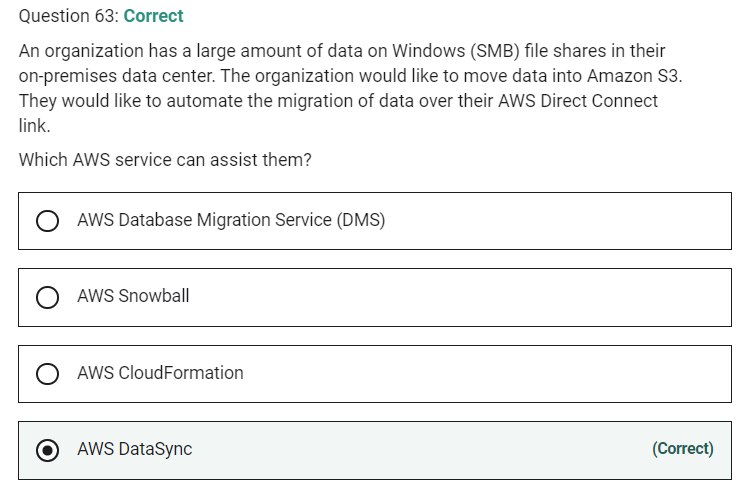
**INCORRECT:** "Migrate the website to Amazon S3. Use cross-Region replication between Regions and a latency-based Route 53 policy" is incorrect. You cannot host dynamic websites on Amazon S3 (static only).

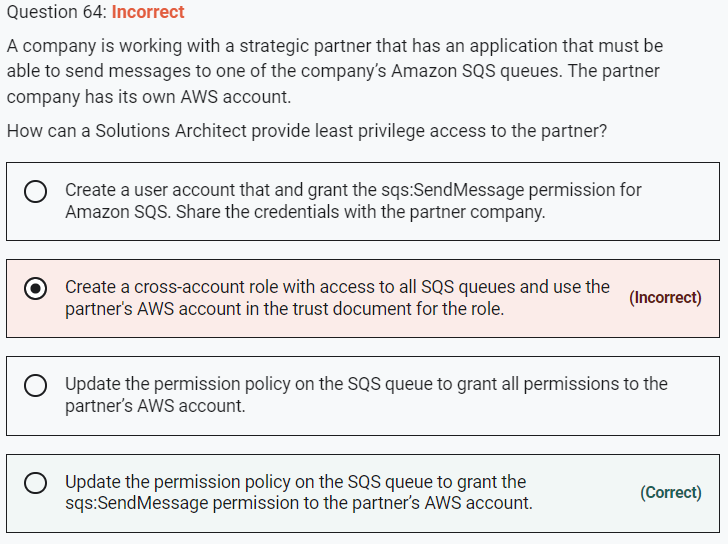












Amazon SQS supports resource-based policies. The best way to grant the permissions using the principle of least privilege is to use a resource-based policy attached to the SQS queue that grants the partner company’s AWS account the sqs:SendMessage privilege.

**INCORRECT:** "Create a user account that and grant the sqs:SendMessage permission for Amazon SQS. Share the credentials with the partner company" is incorrect. This would provide the permissions for all SQS queues, not just the queue the partner company should be able to access.

**INCORRECT:** "Create a cross-account role with access to all SQS queues and use the partner's AWS account in the trust document for the role" is incorrect. This would provide access to all SQS queues and the partner company should only be able to access one SQS queue.

**INCORRECT:** "Update the permission policy on the SQS queue to grant all permissions to the partner’s AWS account" is incorrect. This provides too many permissions; the partner company only needs to send messages to the queue.

