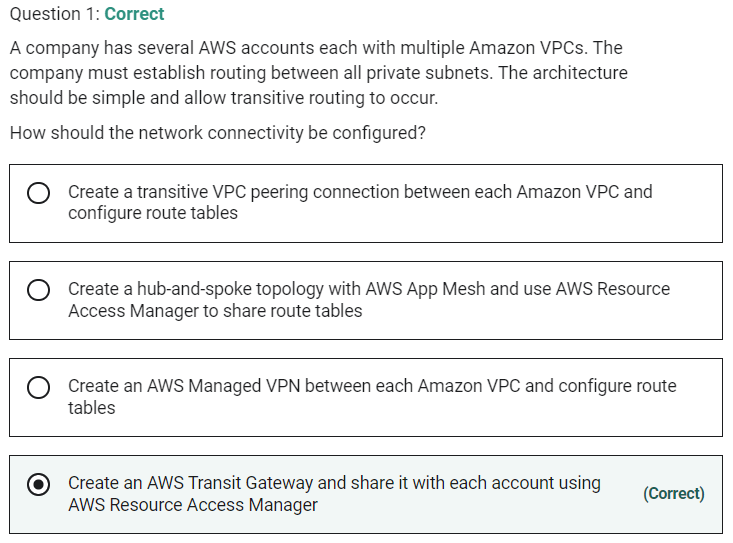
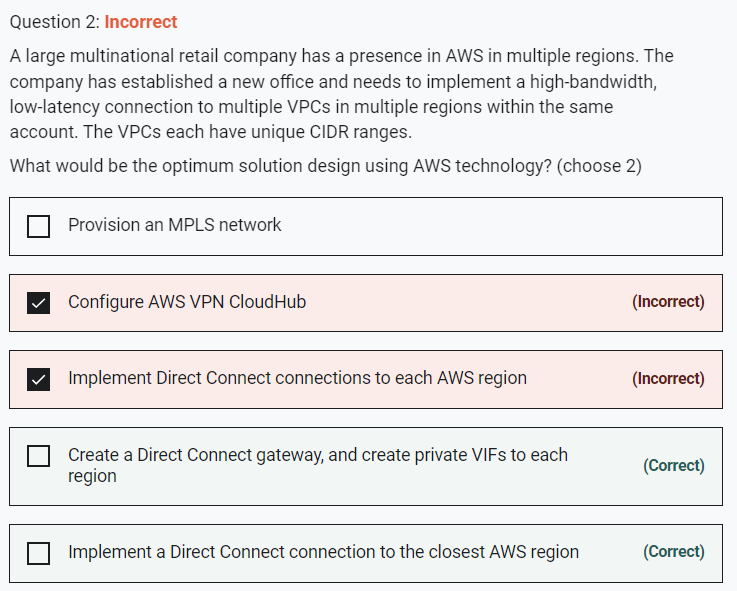
Marked



Marked



The company should implement an AWS Direct Connect connection to the closest region. A Direct Connect gateway can then be used to create private virtual interfaces (VIFs) to each AWS region.

Direct Connect gateway provides a grouping of Virtual Private Gateways (VGWs) and Private Virtual Interfaces (VIFs) that belong to the same AWS account and enables you to interface with VPCs in any AWS Region (except AWS China Region).

You can share a private virtual interface to interface with more than one Virtual Private Cloud (VPC) reducing the number of BGP sessions required.

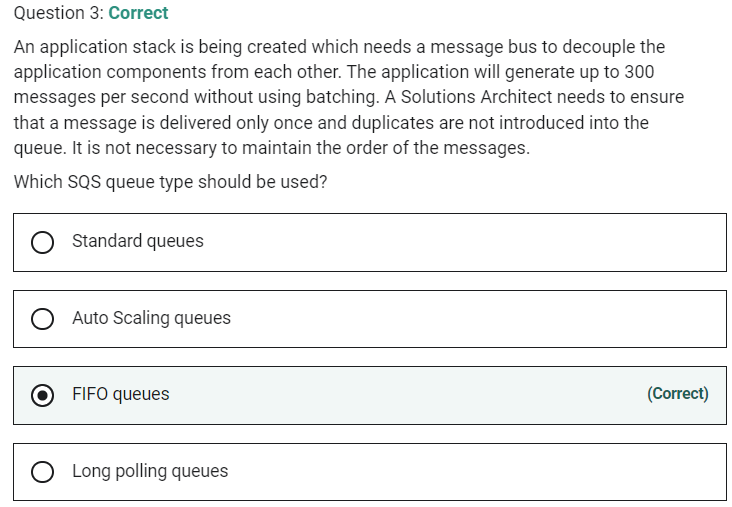
**CORRECT:**"Create a Direct Connect gateway, and create private VIFs to each region" is a correct answer.

**CORRECT:**"Implement a Direct Connect connection to the closest AWS region" is also a correct answer.

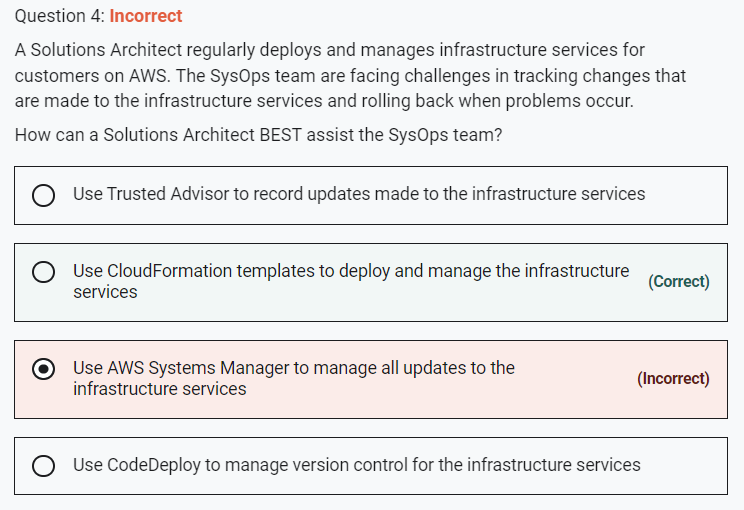
**INCORRECT:** "Configure AWS VPN CloudHub" is incorrect. AWS VPN CloudHub is not the best solution as you have been asked to implement high-bandwidth, low-latency connections and VPN uses the Internet so is not reliable.

**INCORRECT:** "Provision an MPLS network" is incorrect. An MPLS network could be used to create a network topology that gets you closer to AWS in each region but you would still need use Direct Connect or VPN for the connectivity into AWS. Also, the question states that you should use AWS technology and MPLS is not offered as a service by AWS.

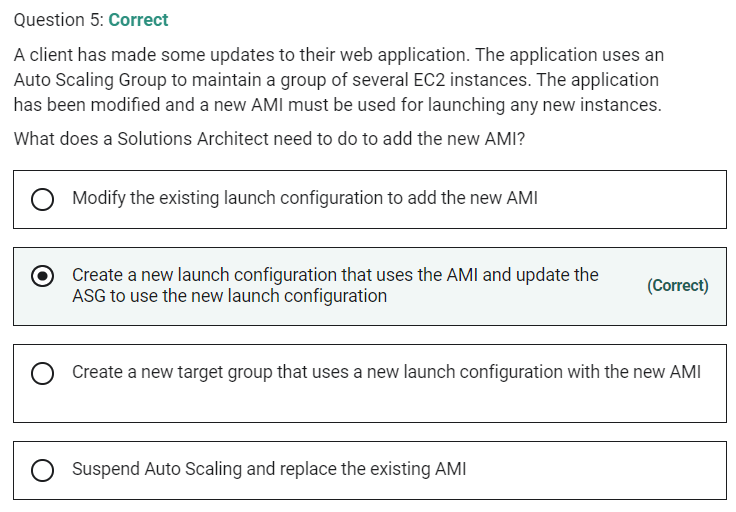
**INCORRECT:** "Implement Direct Connect connections to each AWS region" is incorrect. You do not need to implement multiple Direct Connect connections to each region. This would be a more expensive option as you would need to pay for an international private connection.

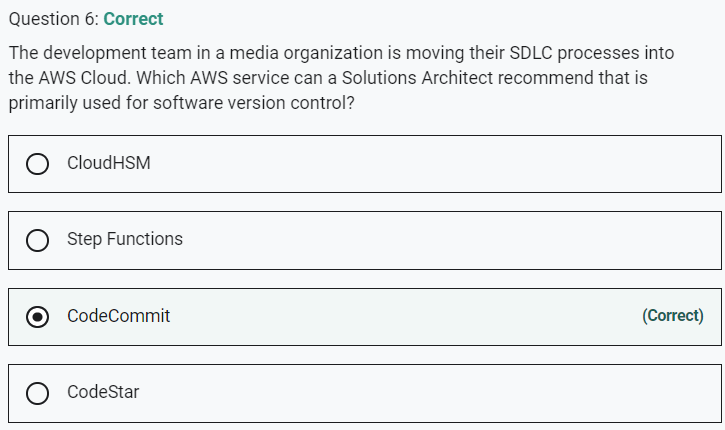


Marked

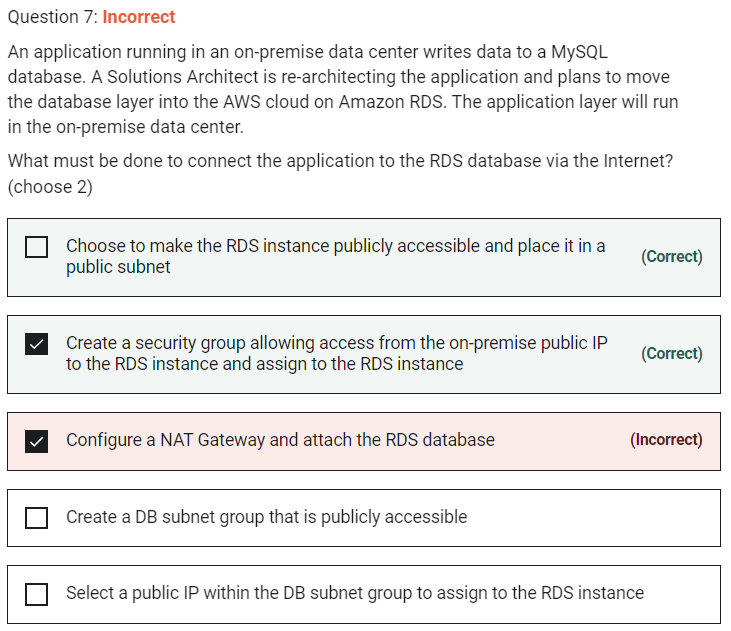


Marked





Marked



When you create the RDS instance, you need to select the option to make it publicly accessible. A security group will need to be created and assigned to the RDS instance to allow access from the public IP address of your application (or firewall).

**CORRECT:**"Choose to make the RDS instance publicly accessible and place it in a public subnet" is a correct answer.

**CORRECT:**"Create a security group allowing access from the on-premise public IP to the RDS instance and assign to the RDS instance" is also a correct answer.

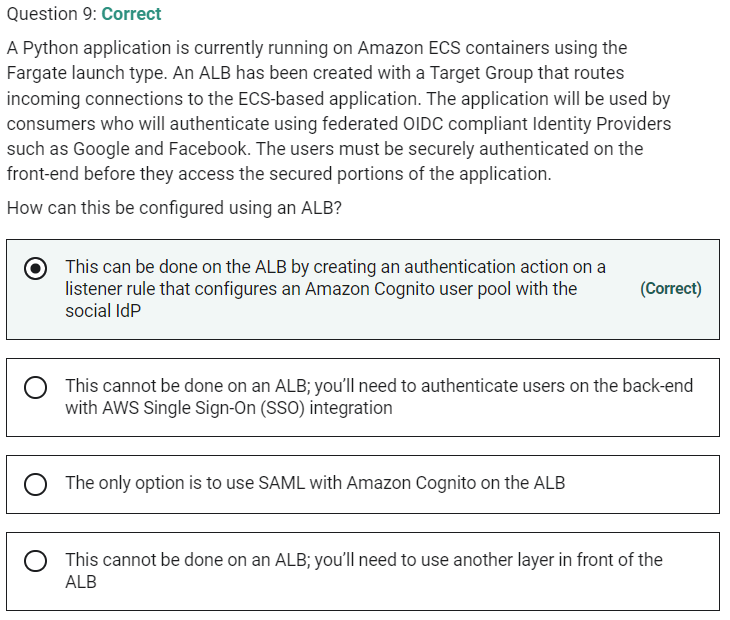
**INCORRECT:** "Configure a NAT Gateway and attach the RDS database" is incorrect. NAT Gateways are used for enabling Internet connectivity for EC2 instances in private subnets.

**INCORRECT:** "Select a public IP within the DB subnet group to assign to the RDS instance" is incorrect. The RDS instance does not require a public IP.

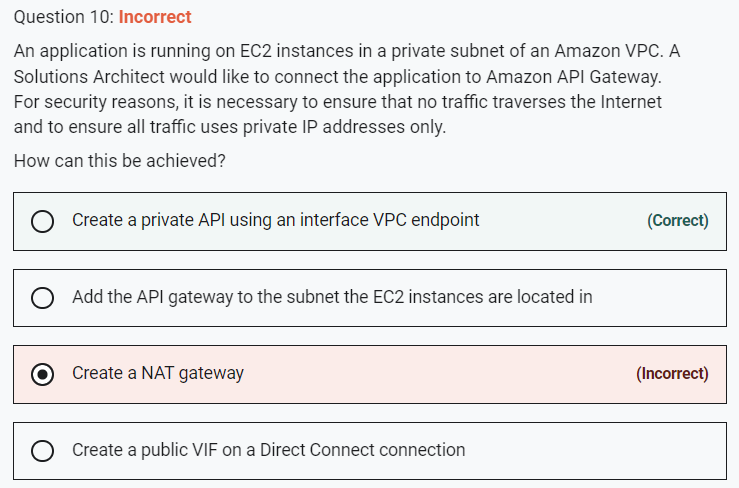
**INCORRECT:** "Create a DB subnet group that is publicly accessible" is incorrect. A DB subnet group is a collection of subnets (typically private) that you create in a VPC and that you then designate for your DB instance. The DB subnet group cannot be made publicly accessible, even if the subnets are public subnets, it is the RDS DB that must be configured to be publicly accessible.



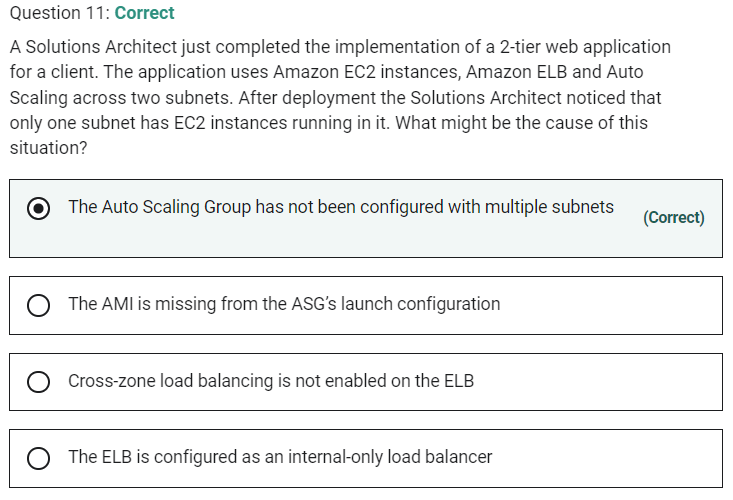
Marked

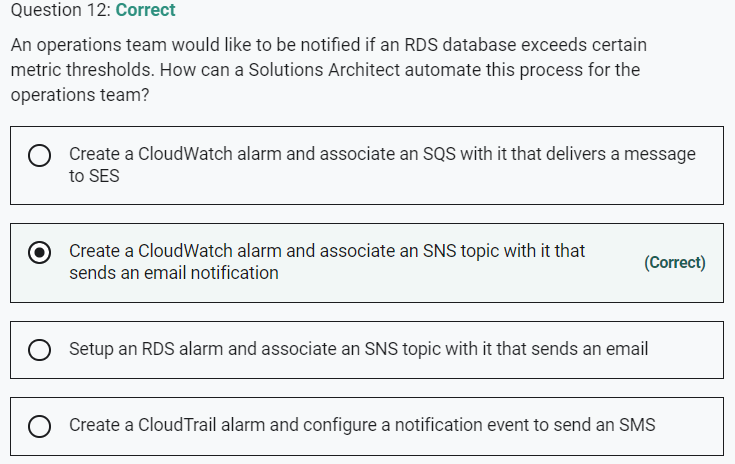


Marked

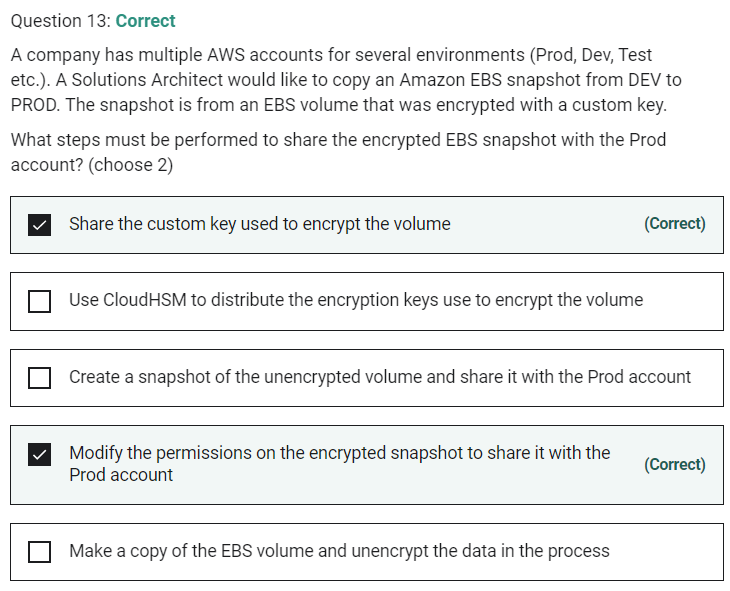


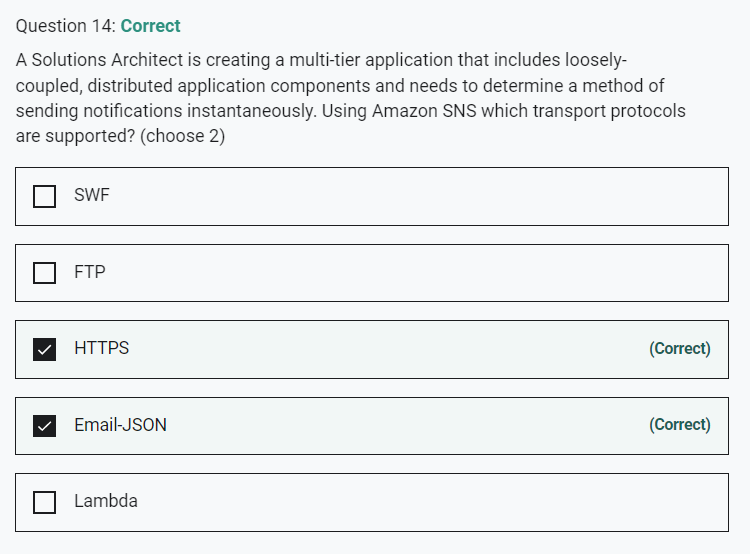
Marked



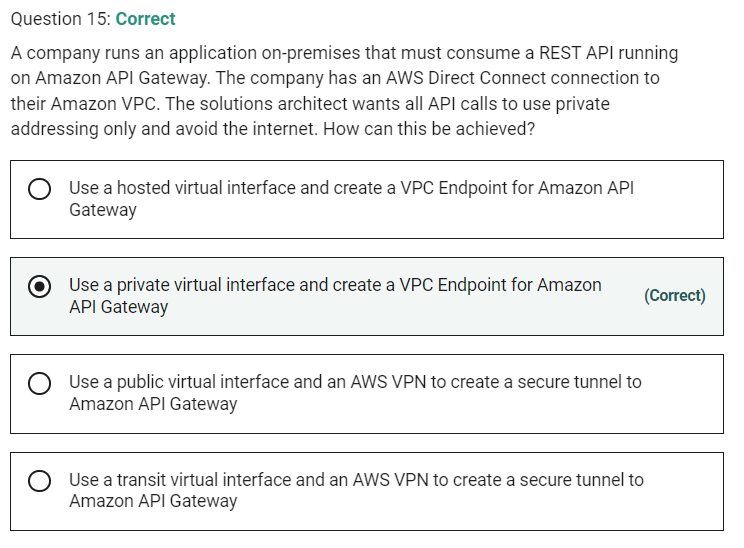


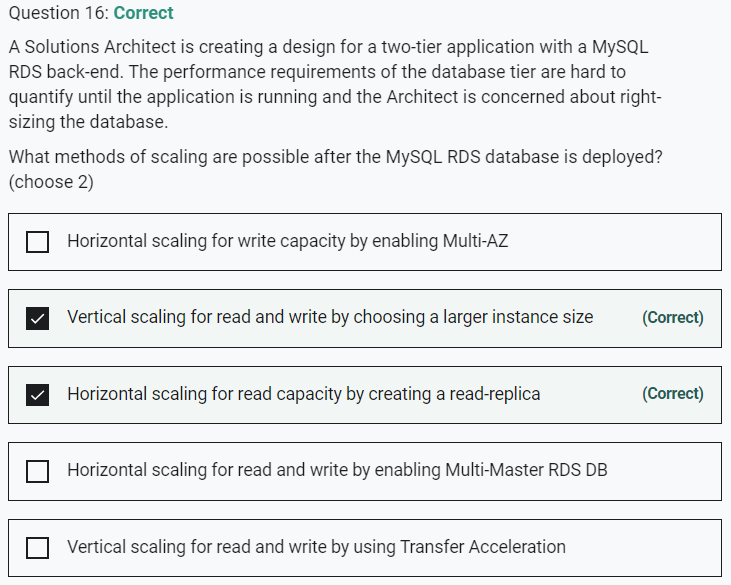
Marked



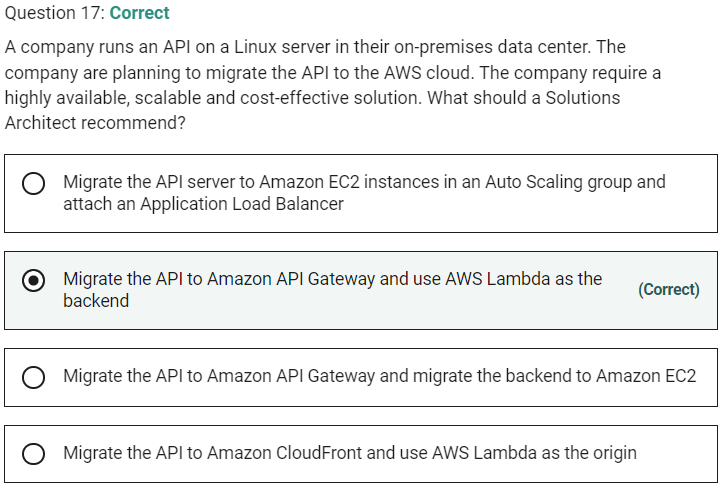


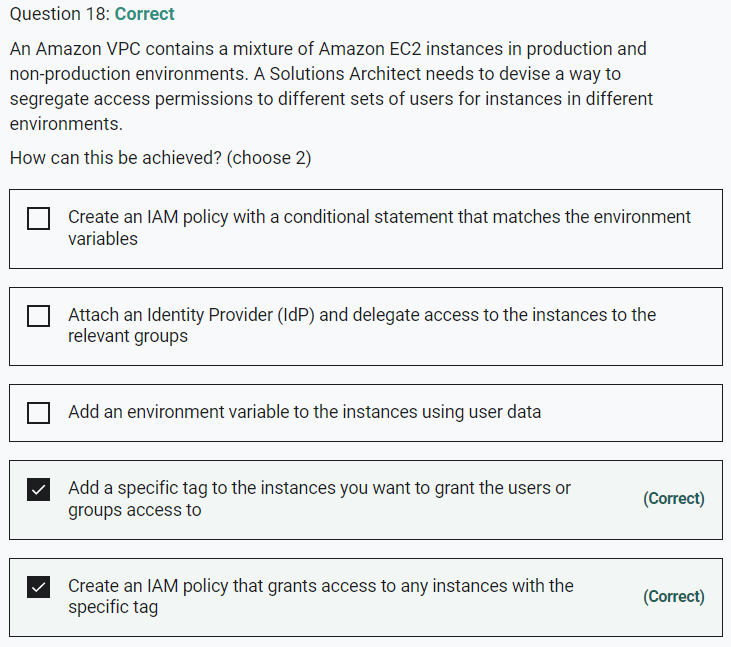
Marked

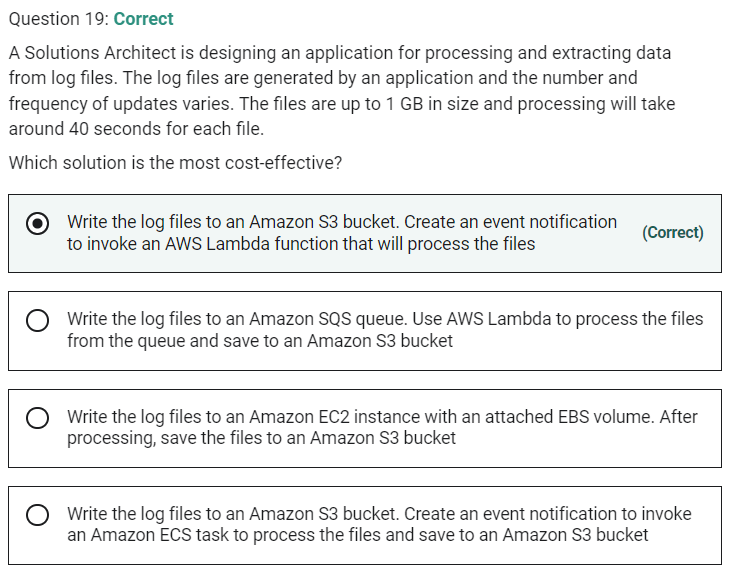




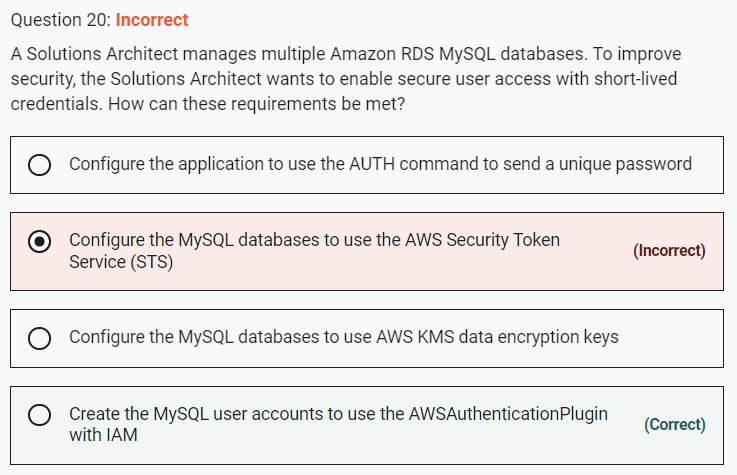
Marked





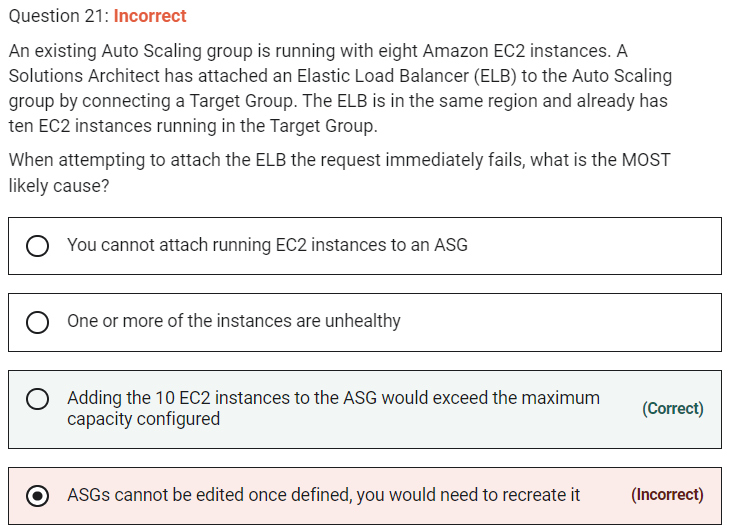


Marked



With MySQL, authentication is handled by AWSAuthenticationPlugin—an AWS-provided plugin

Marked



You can attach one or more Target Groups to your ASG to include instances behind an ALB and the ELBs must be in the same region. Once you do this any EC2 instance existing or added by the ASG will be automatically registered with the ASG defined ELBs. If adding an instance to an ASG would result in exceeding the maximum capacity of the ASG the request will fail.

**CORRECT:**"Adding the 10 EC2 instances to the ASG would exceed the maximum capacity configured" is the correct answer.

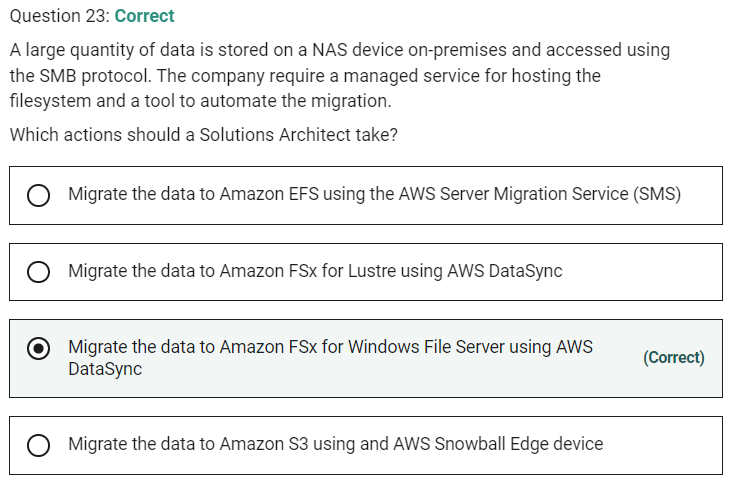
**INCORRECT:** "One or more of the instances are unhealthy" is incorrect. After the load balancer enters the InService state, Amazon EC2 Auto Scaling terminates and replaces any instances that are reported as unhealthy. However, in this case the request immediately failed so having one or more unhealthy instances is not the issue.

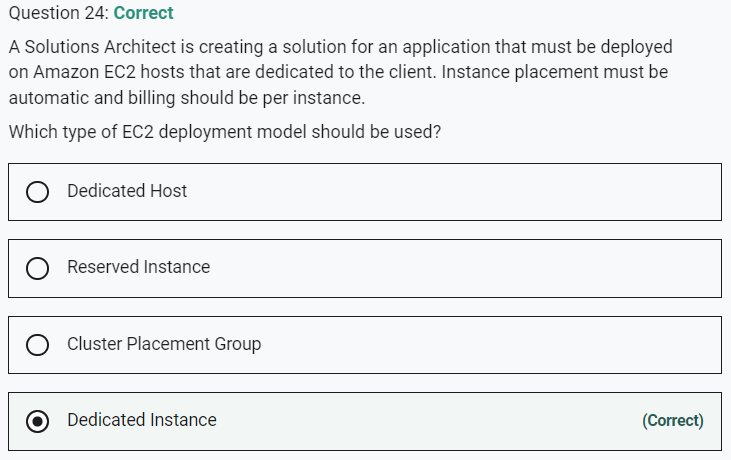
**INCORRECT:** "ASGs cannot be edited once defined, you would need to recreate it" is incorrect. Auto Scaling Groups can be edited once created (however launch configurations cannot be edited).

**INCORRECT:** "You cannot attach running EC2 instances to an ASG" is incorrect. You can attach running EC2 instances to an ASG.

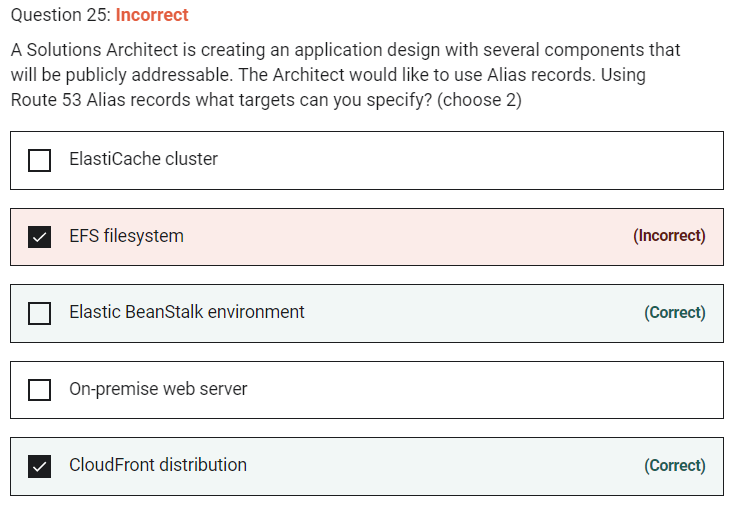
Marked

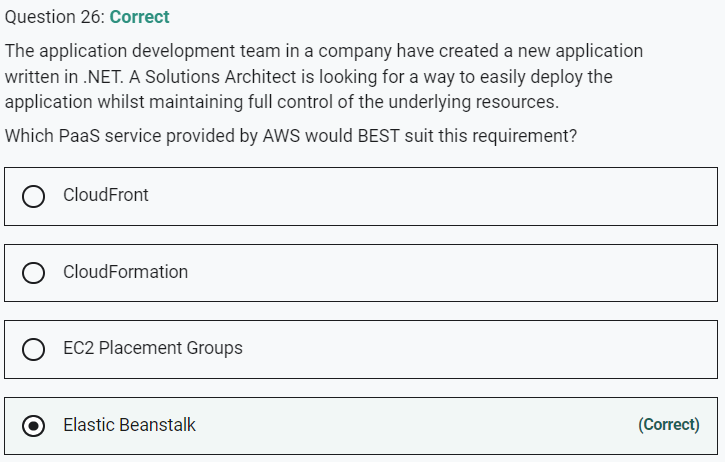


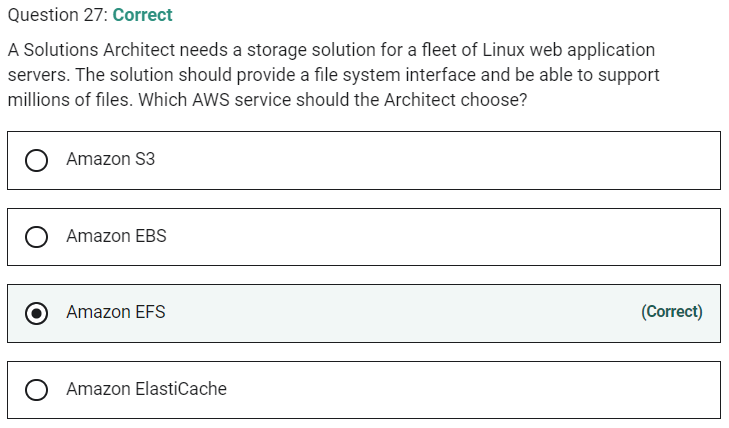


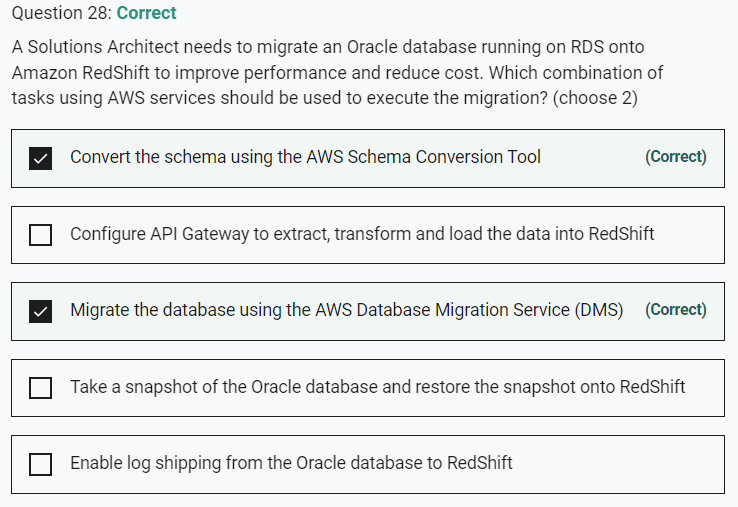


Marked

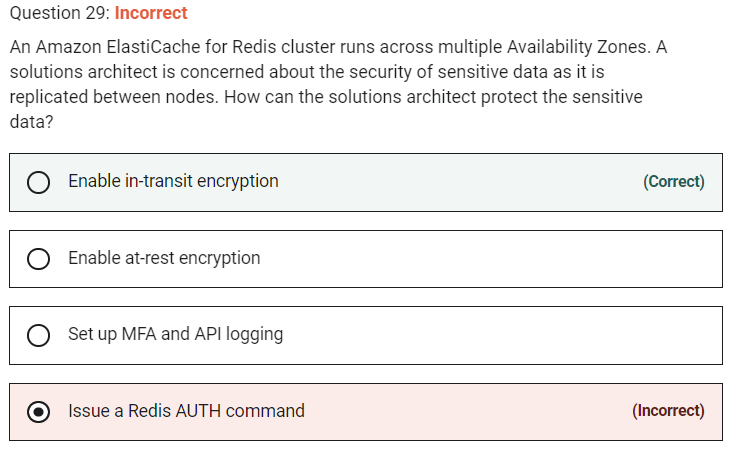


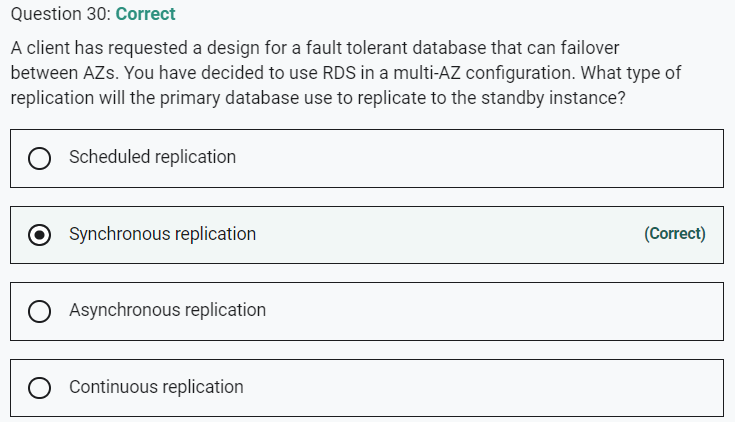


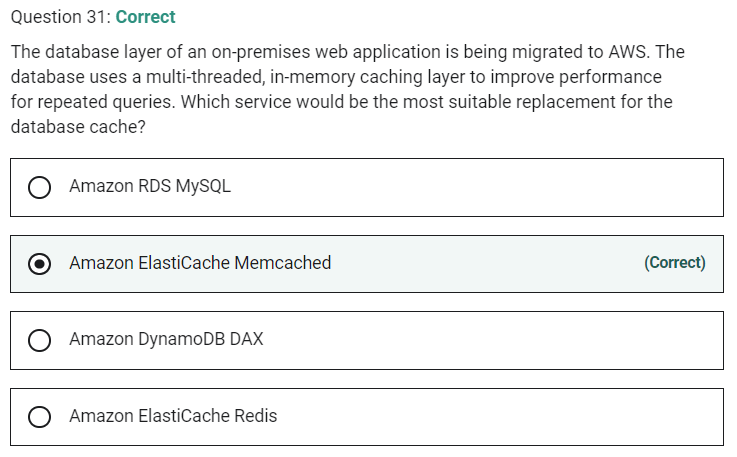


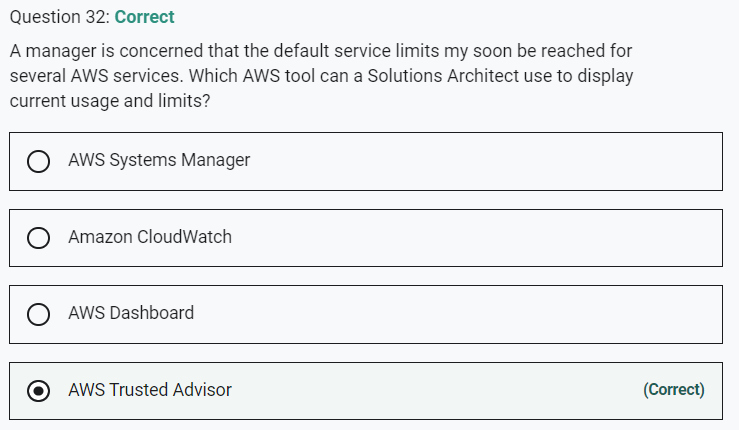


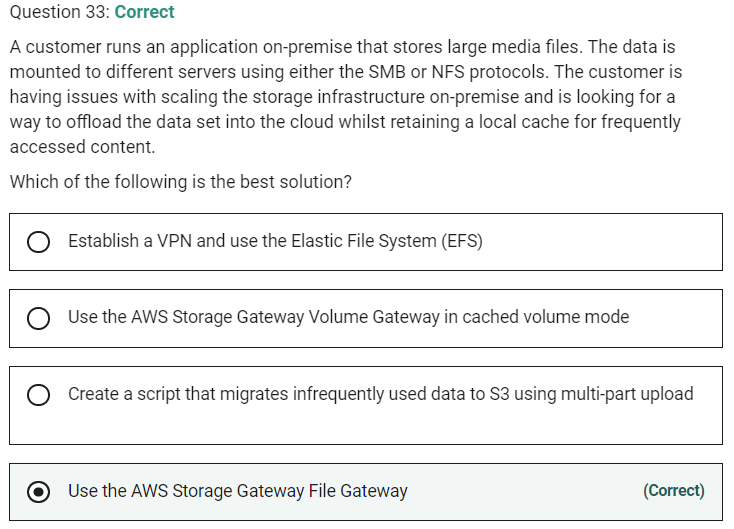
Marked

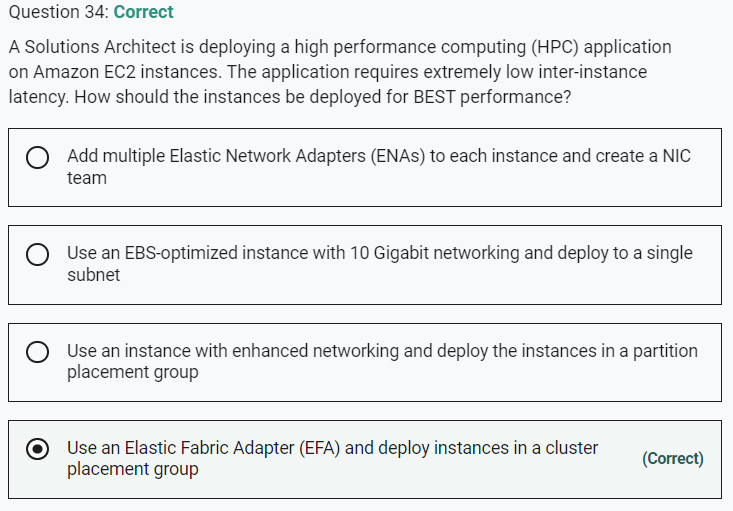




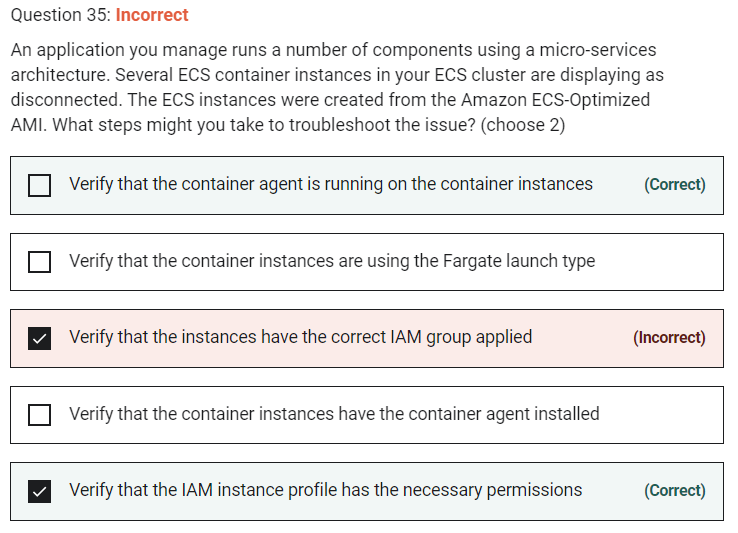








Marked



Troubleshooting steps for containers include:

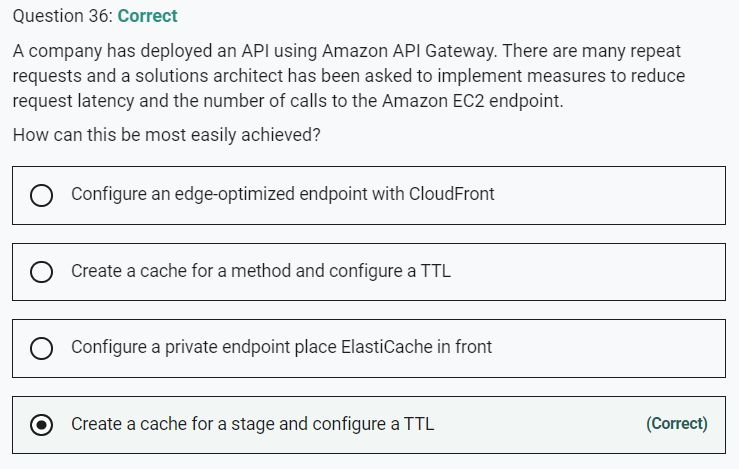
- Verify that the Docker daemon is running on the container instance.

- Verify that the Docker Container daemon is running on the container instance.

- Verify that the container agent is running on the container instance.

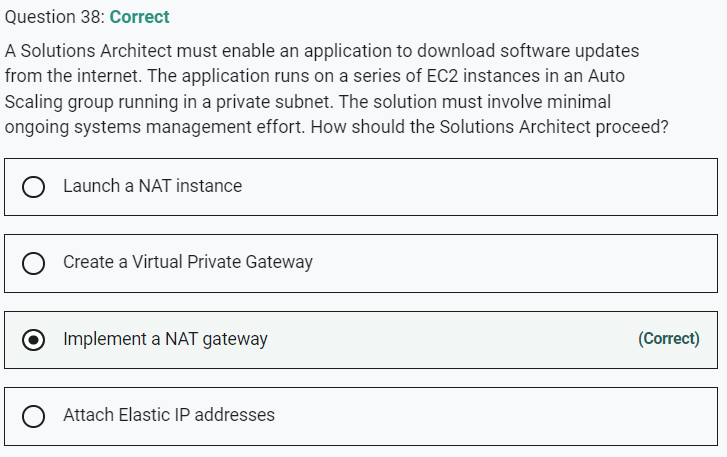
- Verify that the IAM instance profile has the necessary permissions.

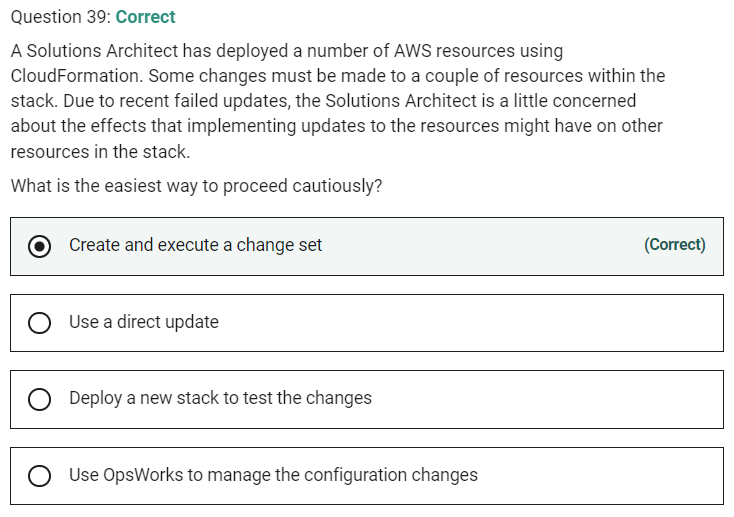
Marked



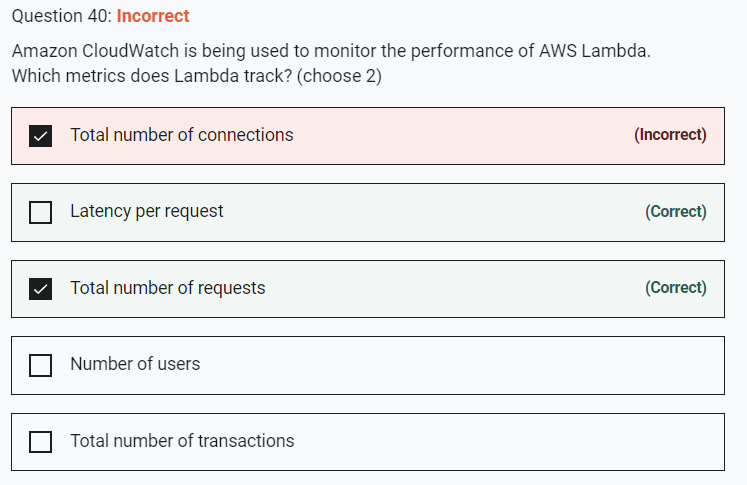
 An API cache is not enabled for a method, it is enabled for a stage.



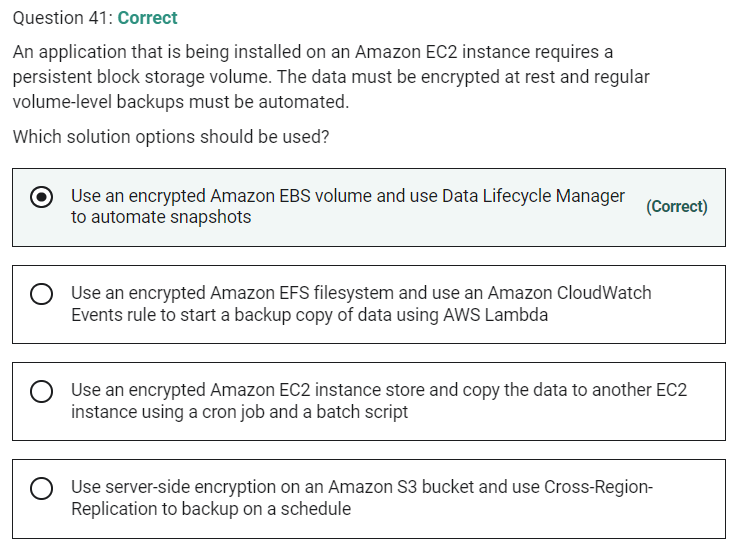


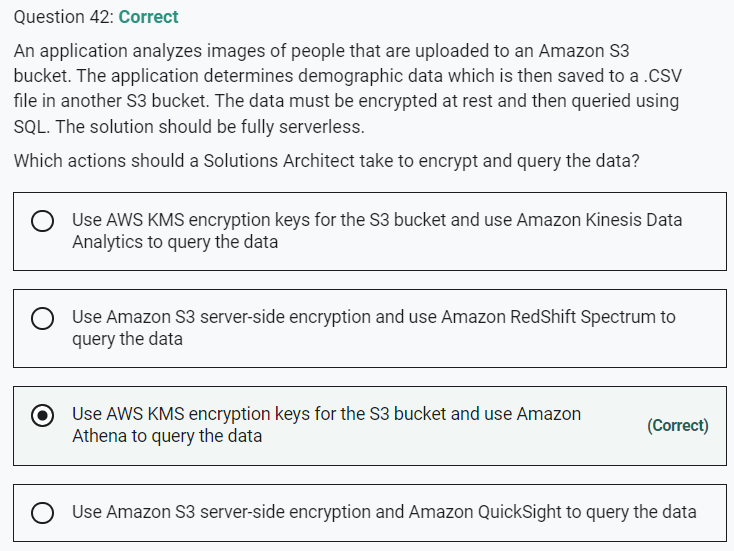


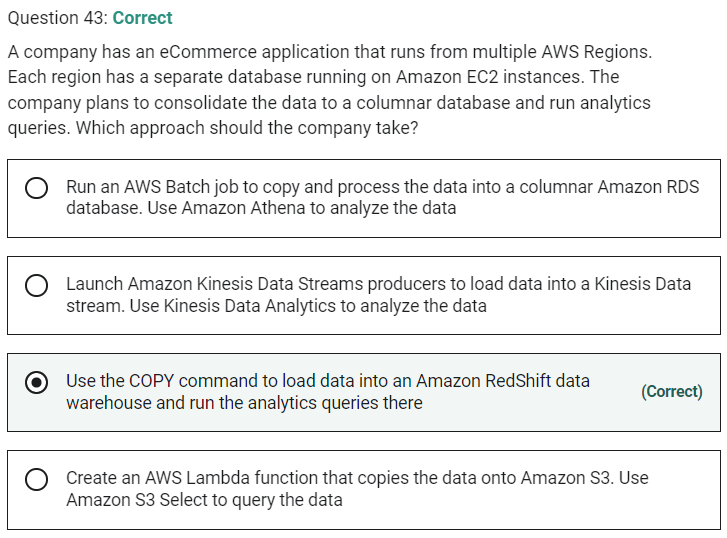
Marked



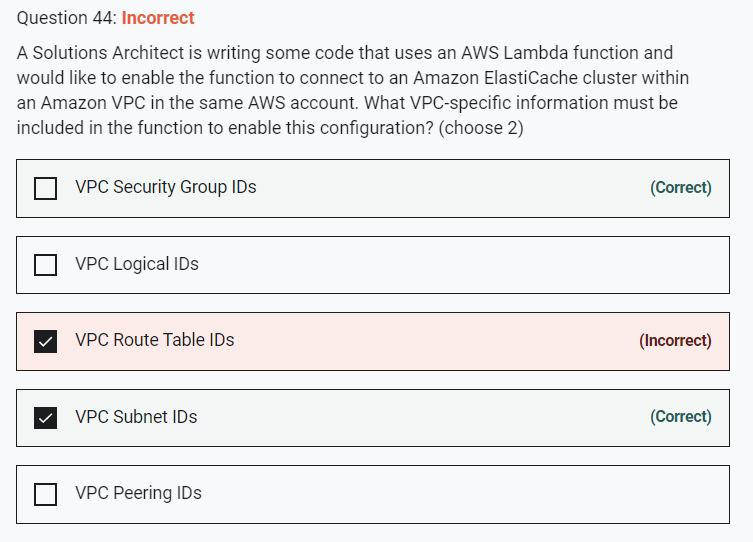
 Lambda tracks the number of requests, the latency per request, and the number of requests resulting in an error. You can view the request rates and error rates using the AWS Lambda Console, the CloudWatch console, and other AWS resources.





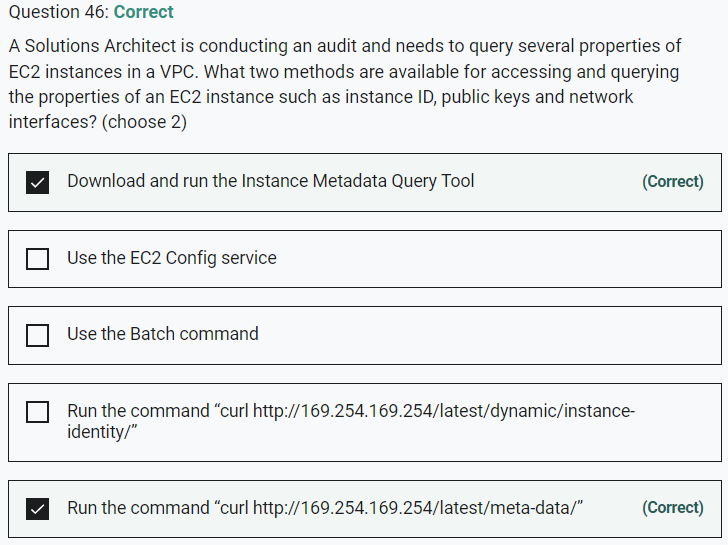


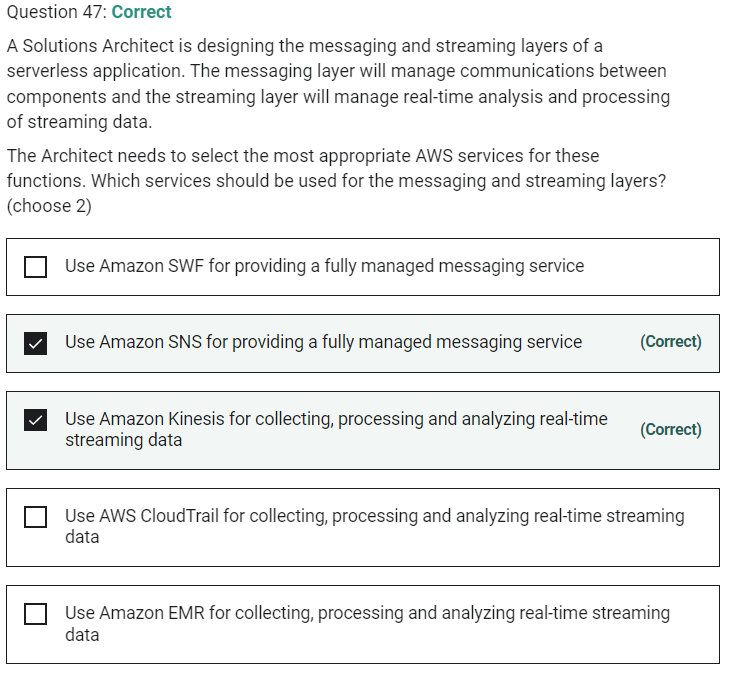
Marked



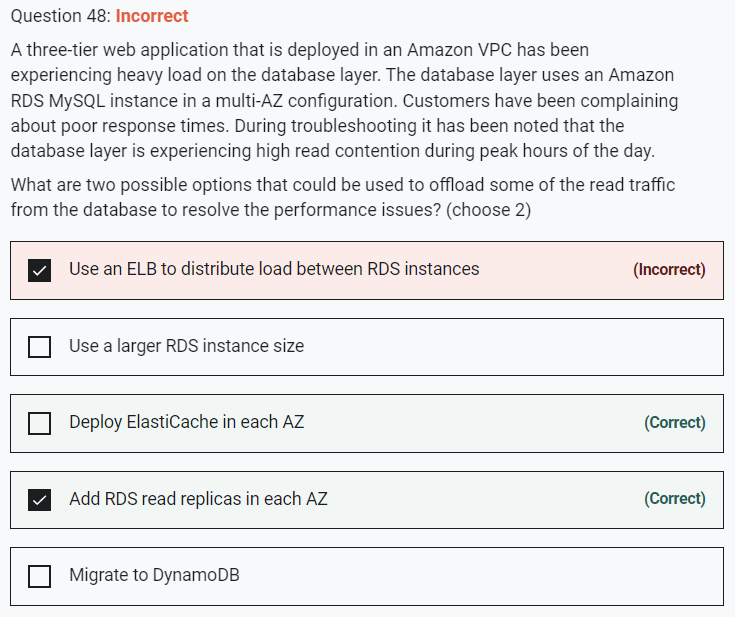
To enable your Lambda function to access resources inside your private VPC, you must provide additional VPC-specific configuration information that includes VPC subnet IDs and security group IDs.



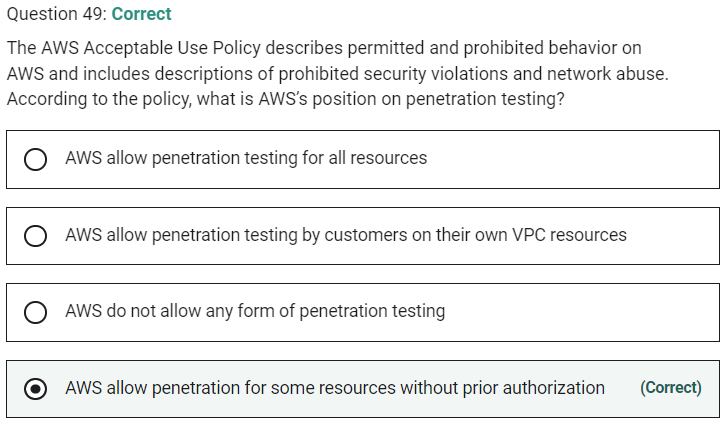


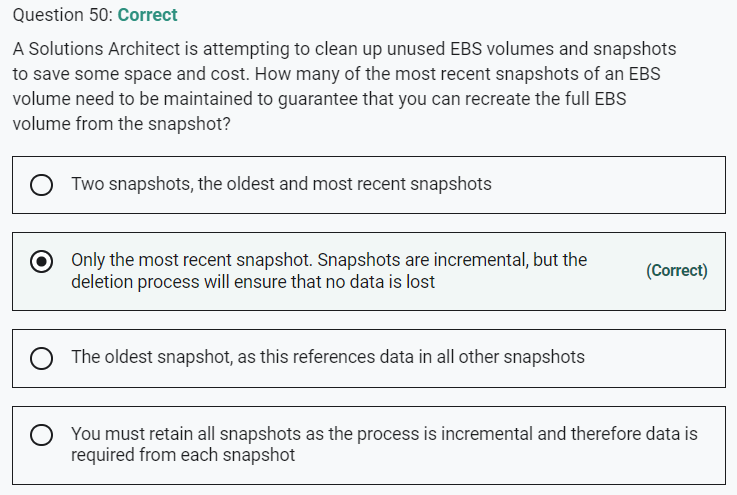


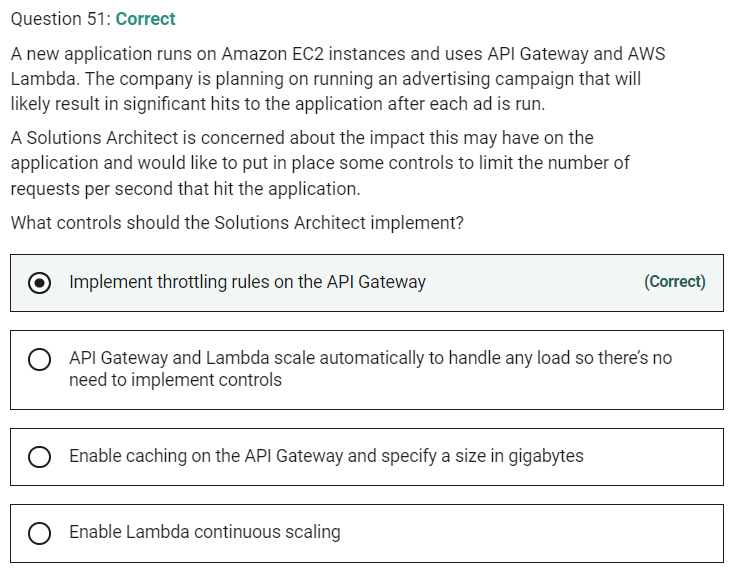
Marked



You cannot use an ELB to distributed load between different RDS instances.

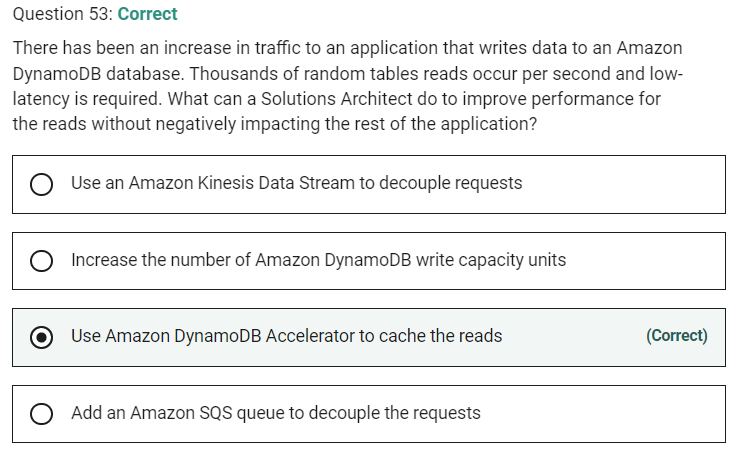




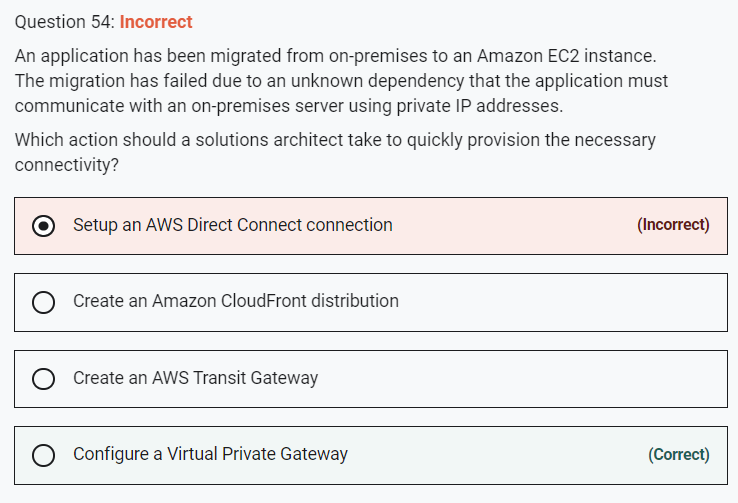


Marked

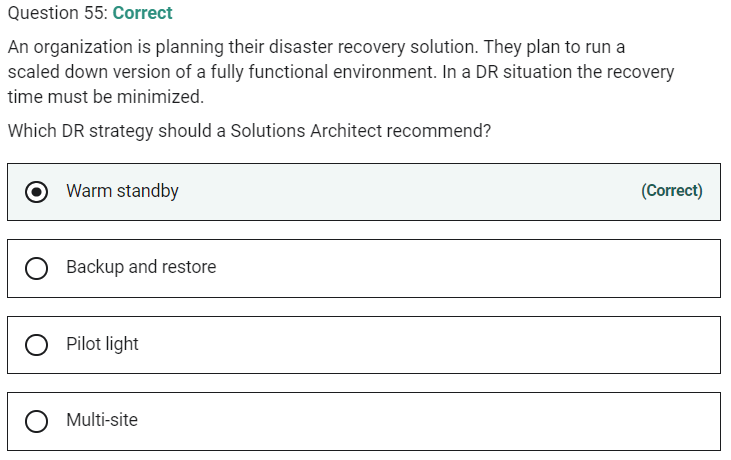


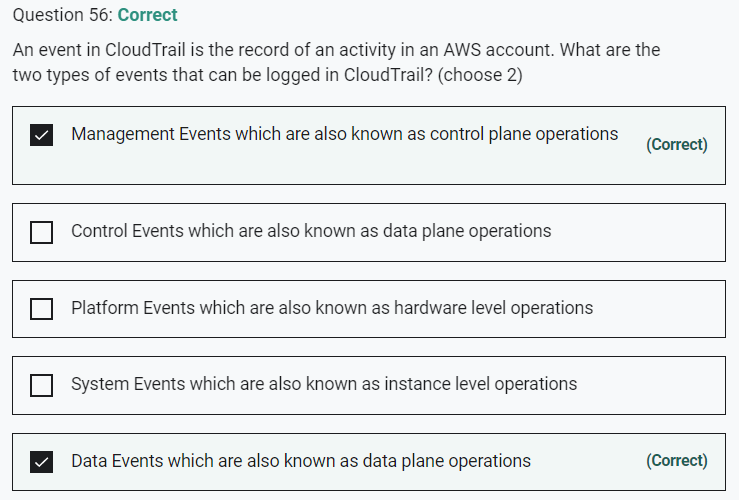


Marked

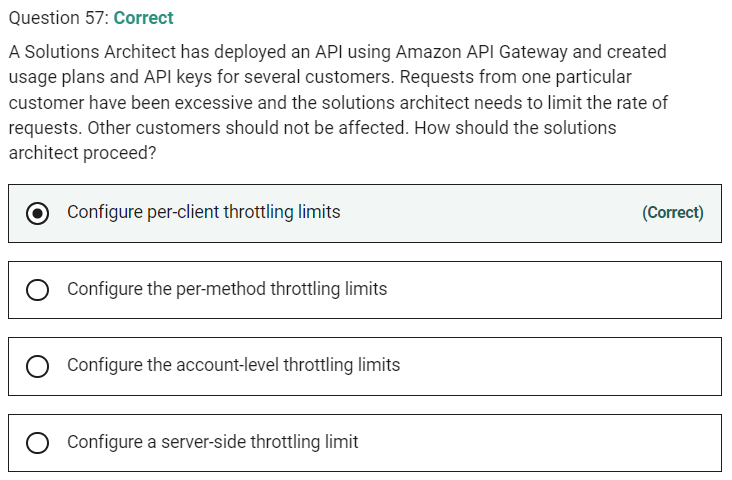


**INCORRECT:** "Setup an AWS Direct Connect connection" is incorrect as this would take too long to provision.

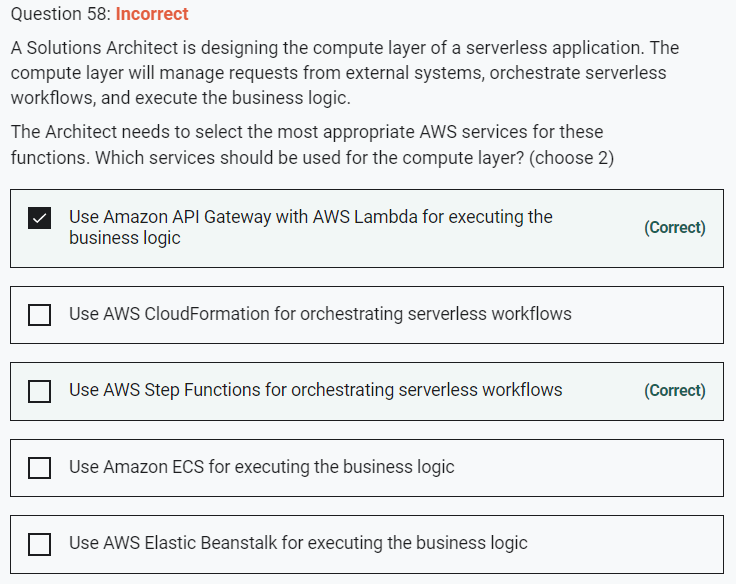


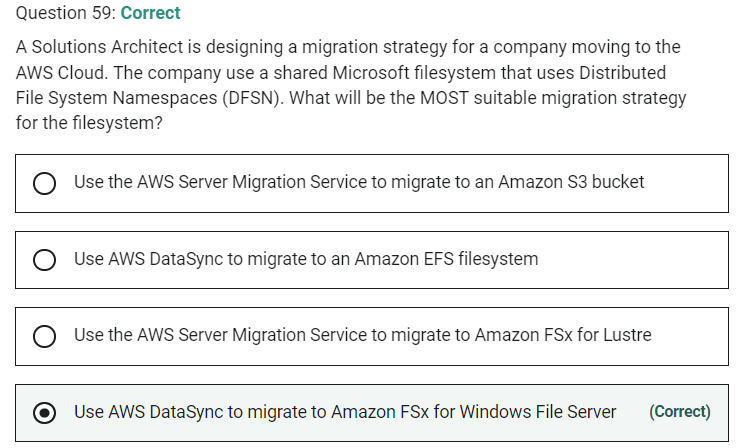


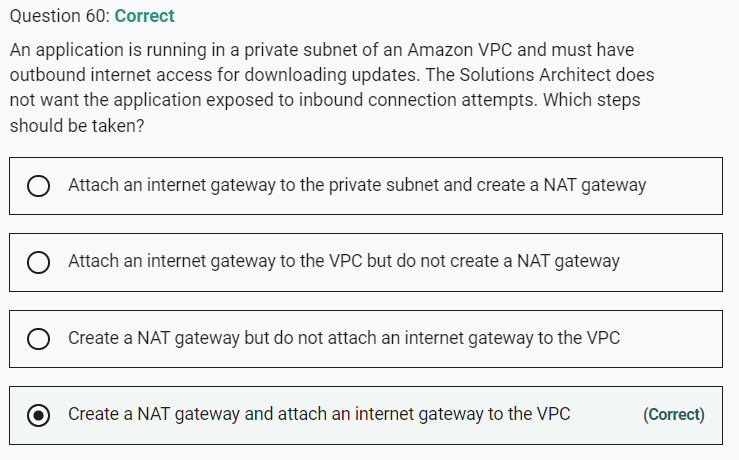
Marked

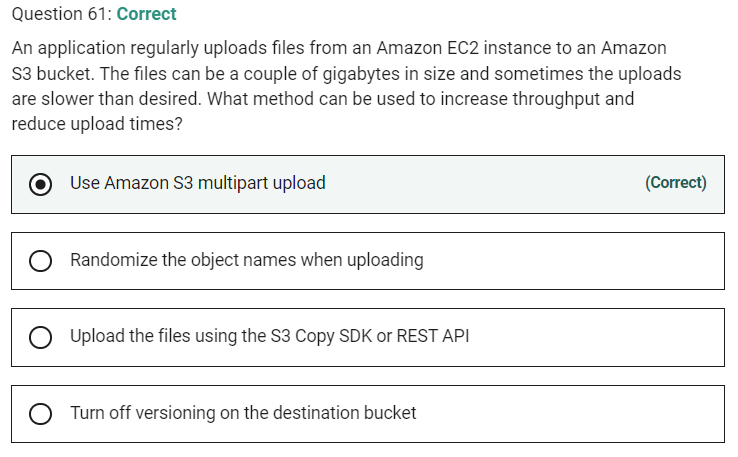


Marked

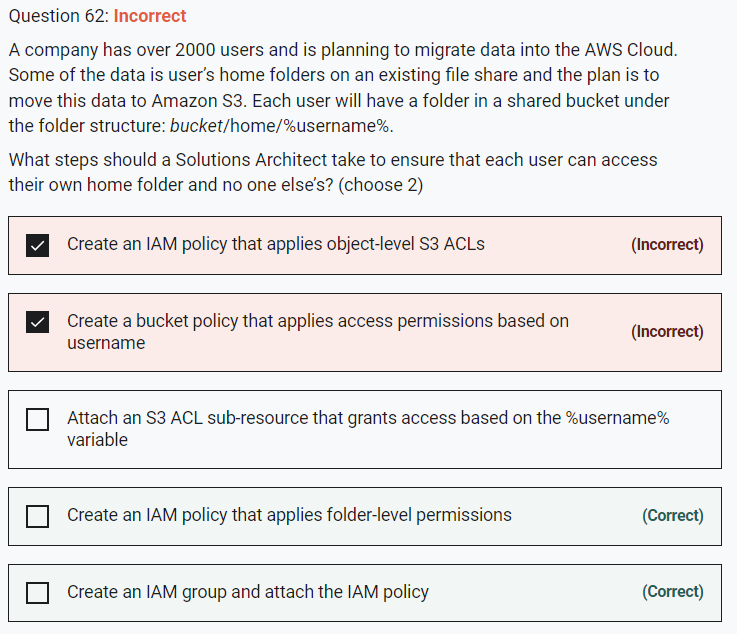




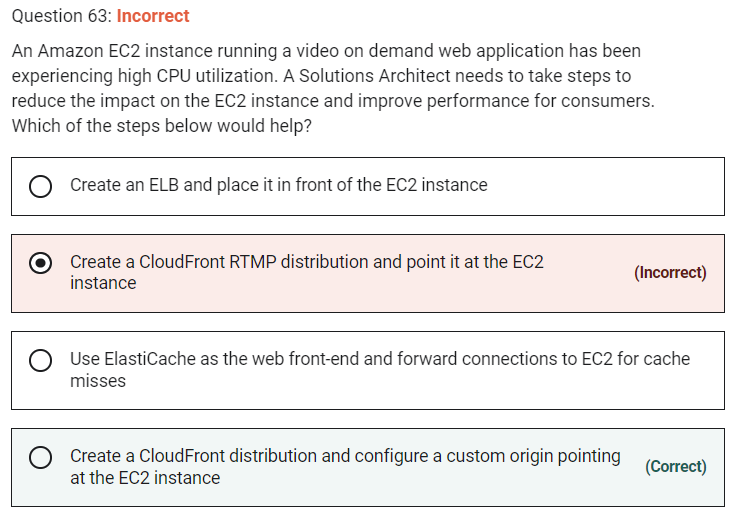




Marked

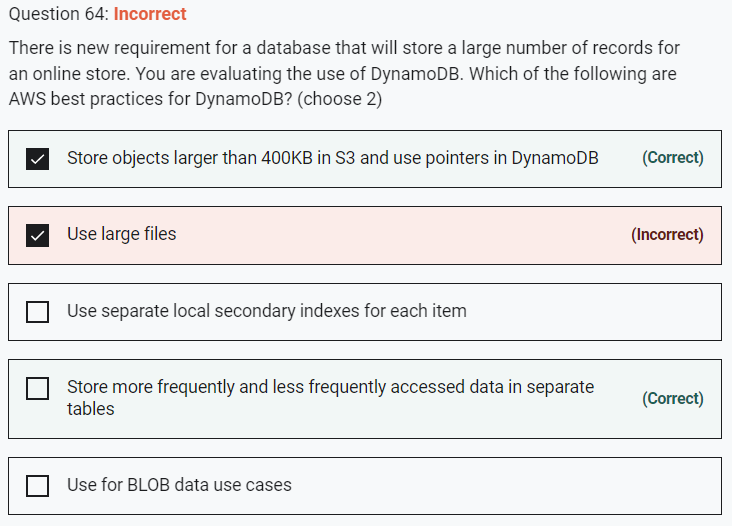


Marked



**INCORRECT:** "Create a CloudFront RTMP distribution and point it at the EC2 instance" is incorrect. For RTMP CloudFront distributions files must be stored in an S3 bucket.

Marked



DynamoDB best practices include:

- Keep item sizes small.

- If you are storing serial data in DynamoDB that will require actions based on data/time use separate tables for days, weeks, months.

- Store more frequently and less frequently accessed data in separate tables.

- If possible compress larger attribute values.

- Store objects larger than 400KB in S3 and use pointers (S3 Object ID) in DynamoDB.

Marked

