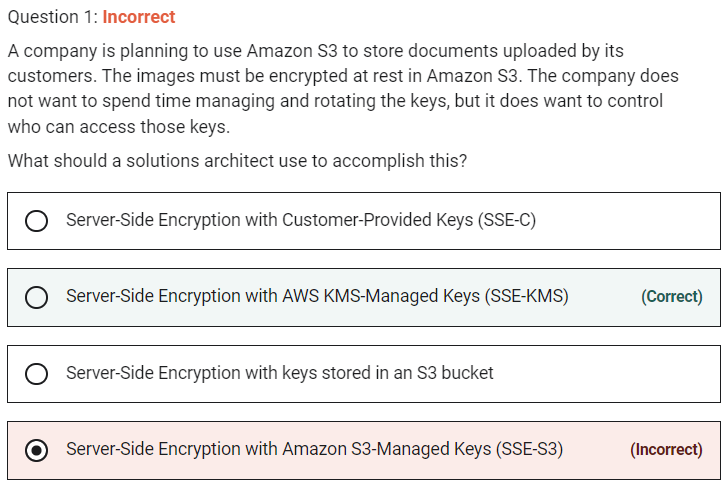
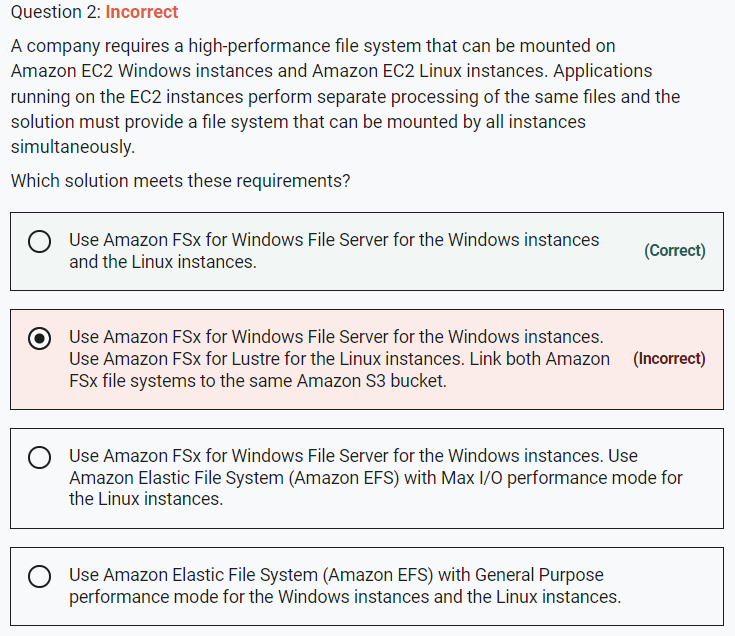
Marked

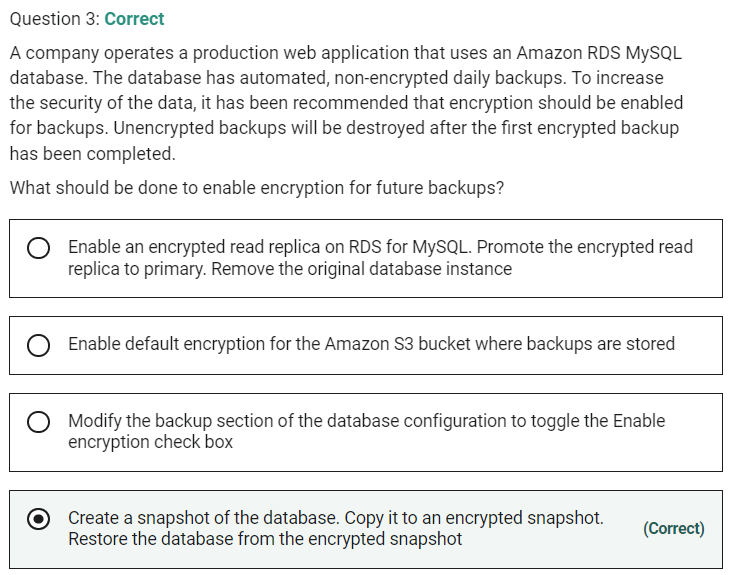


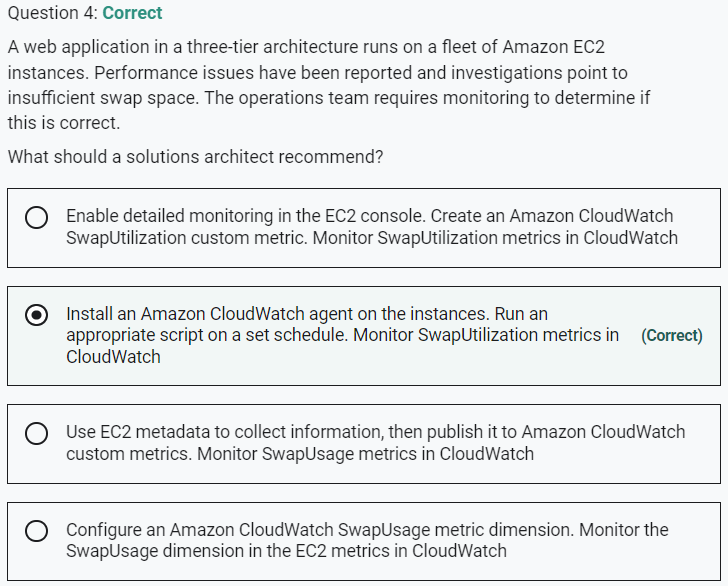
Marked



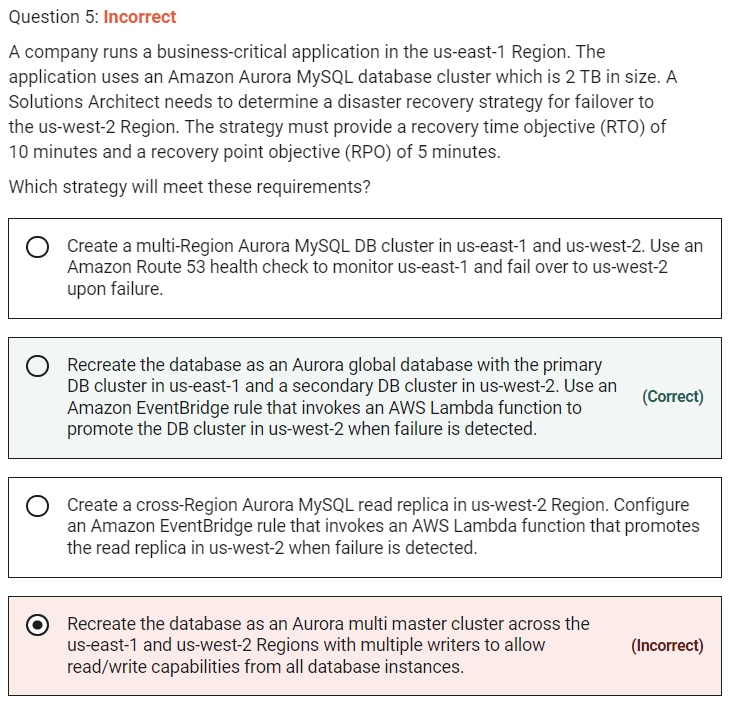
Amazon FSx for windows works for both windows and linux

EFS works only for linux

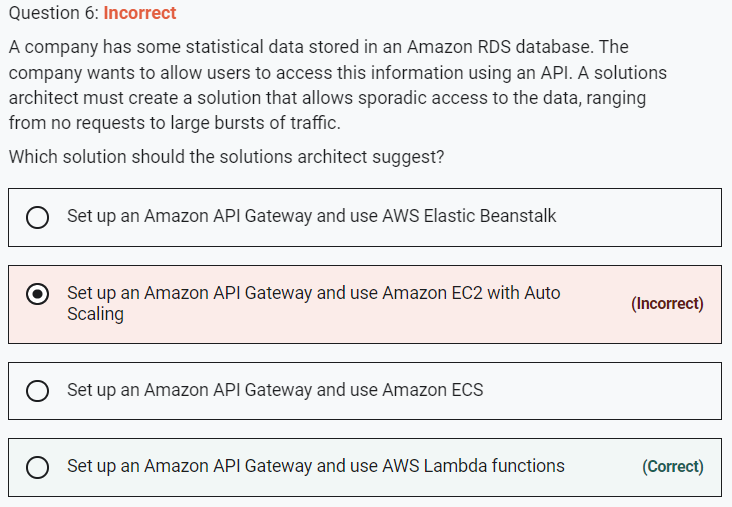




Marked

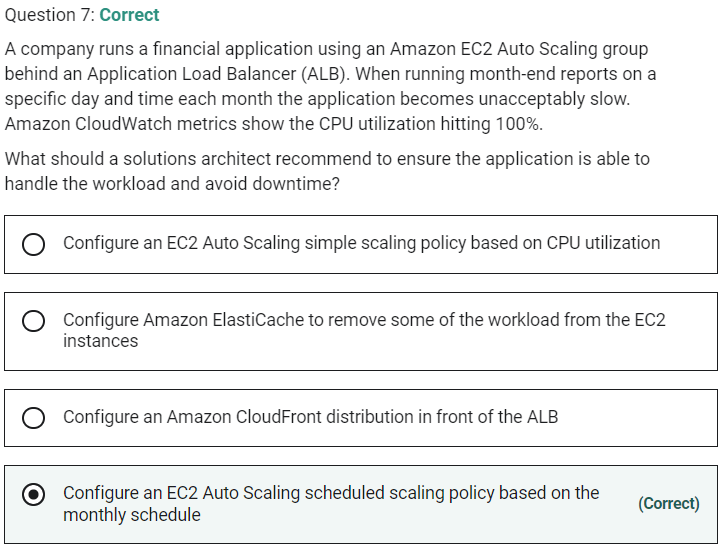


Marked



This question is simply asking you to work out the best compute service for the stated requirements. The key requirements are that the compute service should be suitable for a workload that can range quite broadly in demand from no requests to large bursts of traffic.

AWS Lambda is an ideal solution as you pay only when requests are made and it can easily scale to accommodate the large bursts in traffic. Lambda works well with both API Gateway and Amazon RDS.



Marked



Use CloudWatch Container Insights to collect, aggregate, and summarize metrics and logs from your containerized applications and microservices. Container Insights is available for Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS), and Kubernetes platforms on Amazon EC2.

With Container Insights for EKS you can see the top contributors by memory or CPU, or the most recently active resources. This is available when you select any of the following dashboards in the drop-down box near the top of the page:

  •  ECS Services

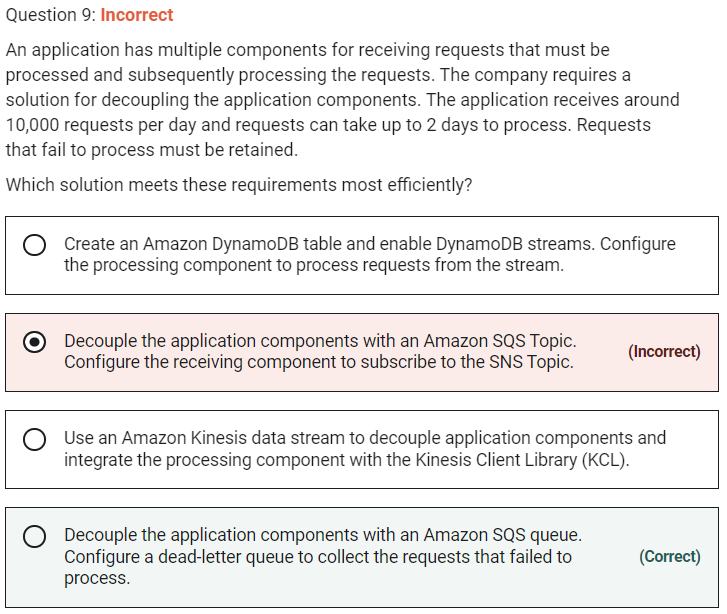
  •  ECS Tasks

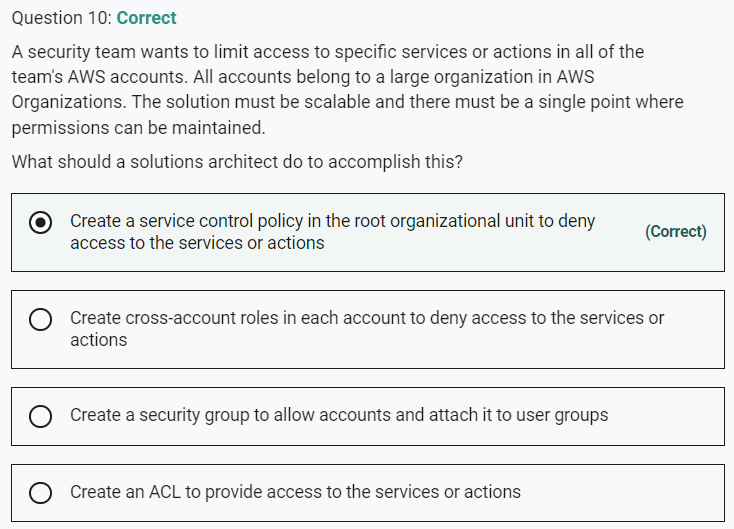
  •  EKS Namespaces

  •  EKS Services

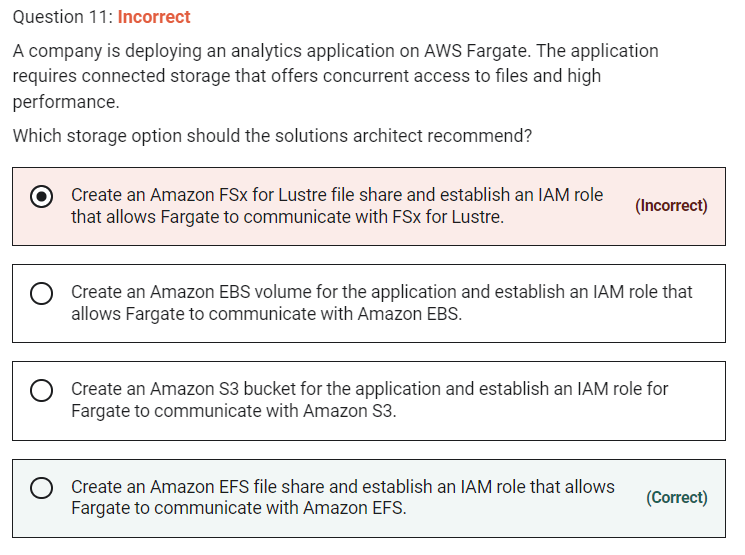
  •  EKS Pods

Marked

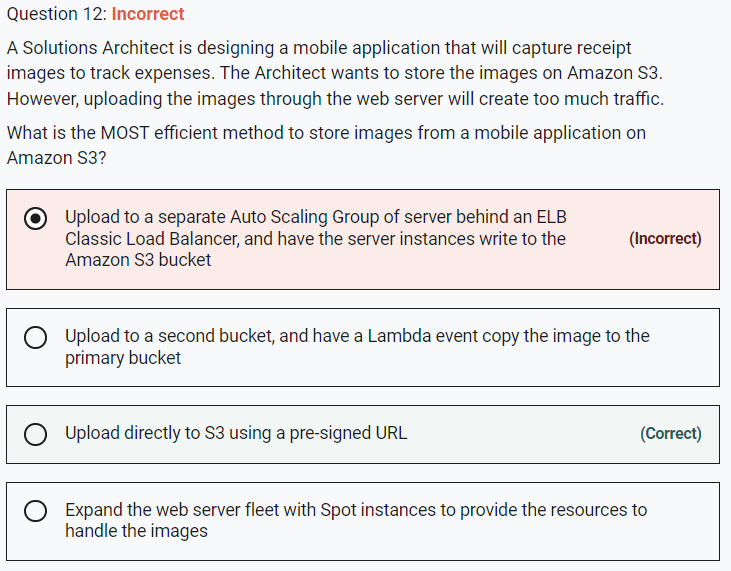




Marked

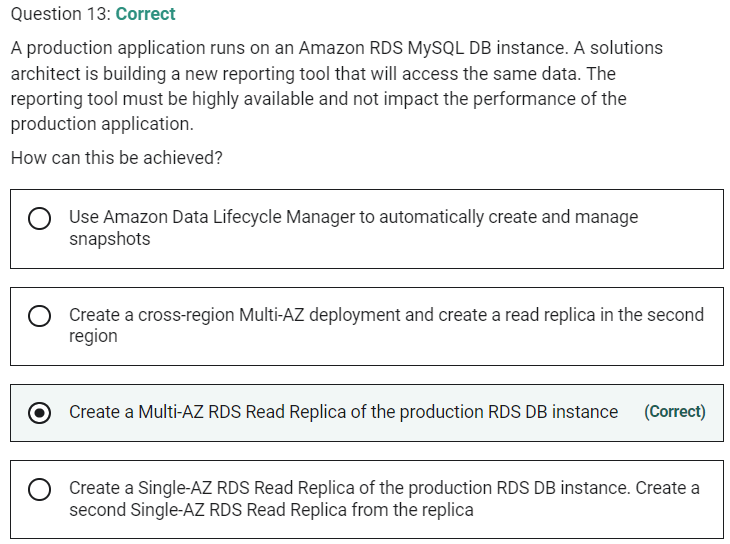


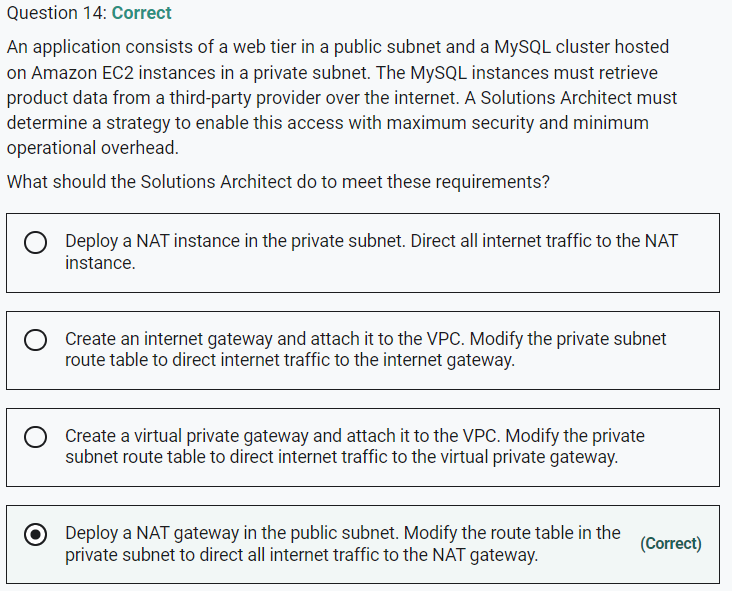
Marked



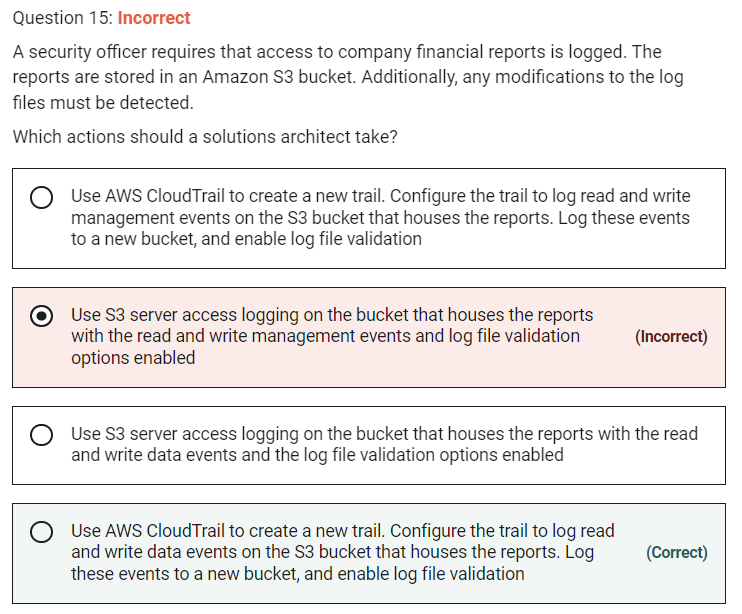
Uploading using a pre-signed URL allows you to upload the object without having any AWS security credentials/permissions. Pre-signed URLs can be generated programmatically and anyone who receives a valid pre-signed URL can then programmatically upload an object. This solution bypasses the web server avoiding any performance bottlenecks.

Marked



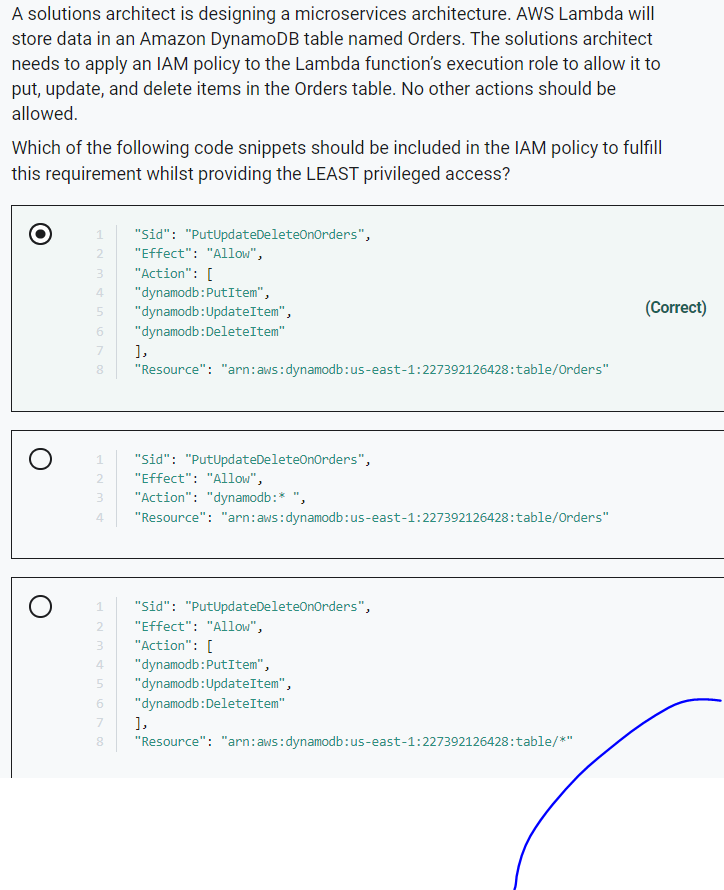


Marked

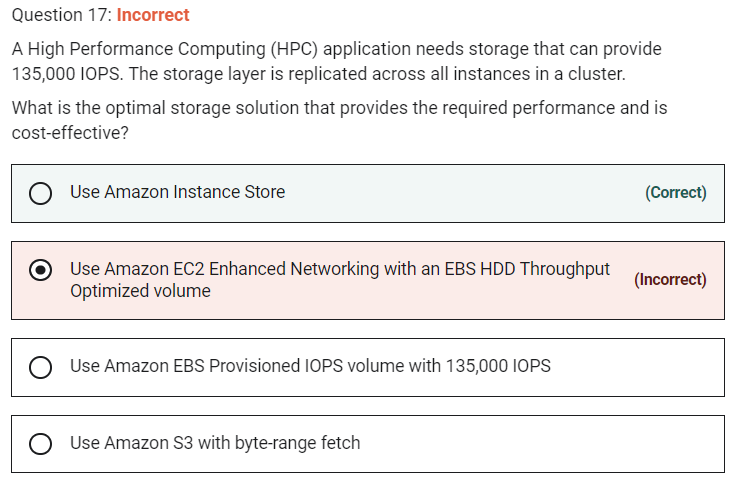


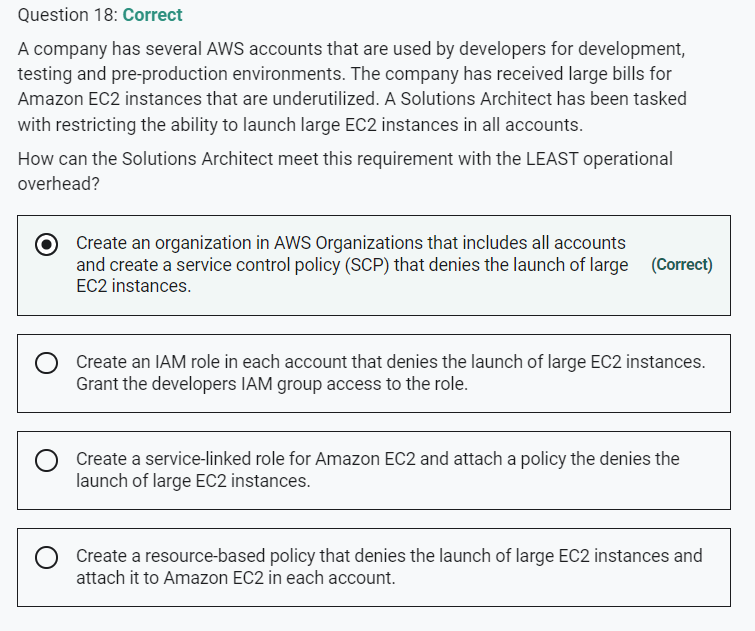
**INCORRECT:** "Use AWS CloudTrail to create a new trail. Configure the trail to log read and write management events on the S3 bucket that houses the reports. Log these events to a new bucket, and enable log file validation" is incorrect as data events should be logged rather than management events.

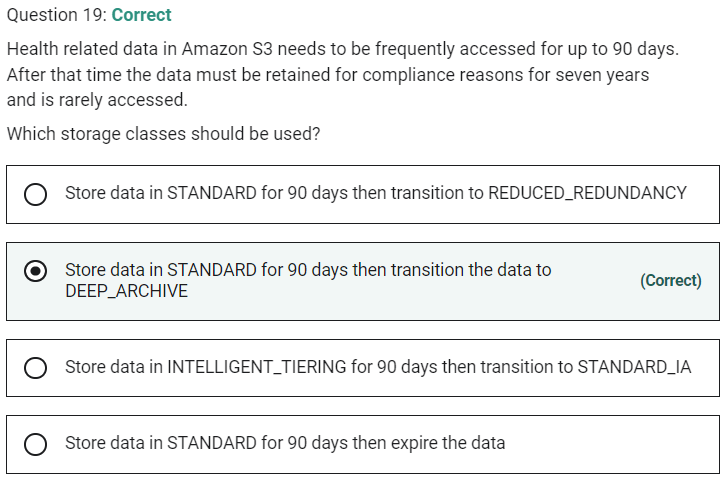
**INCORRECT:** "Use S3 server access logging on the bucket that houses the reports with the read and write data events and the log file validation options enabled" is incorrect as server access logging does not have an option for choosing data events or log file validation.



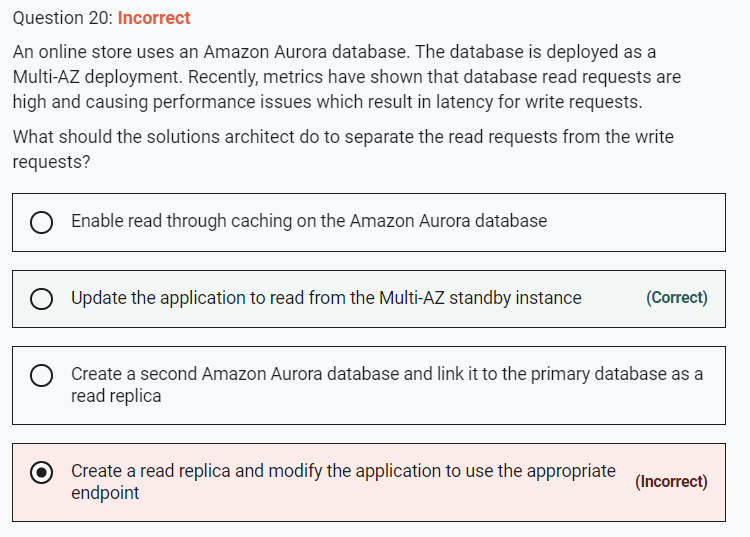
Marked

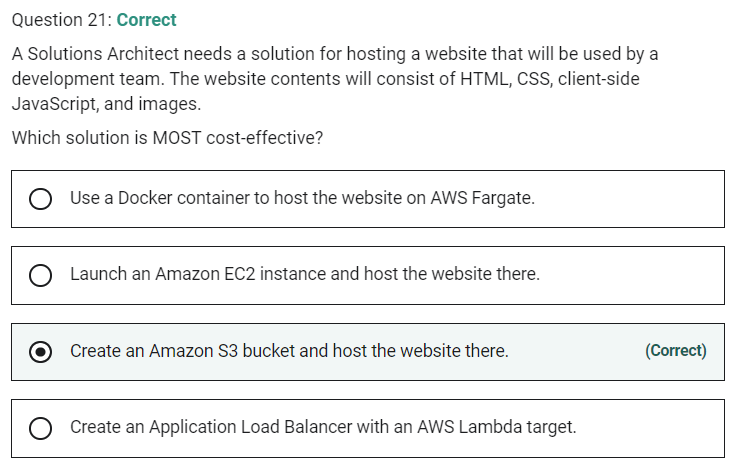






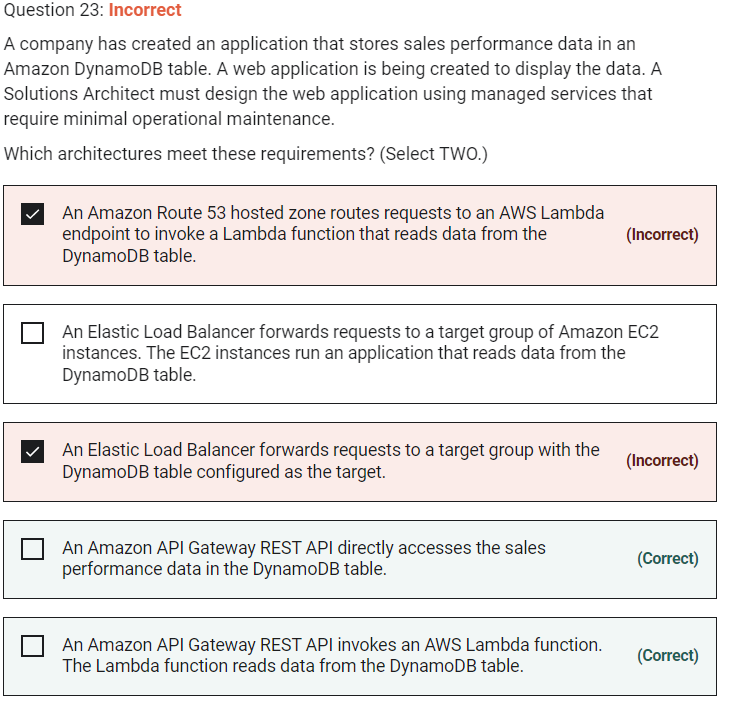
Marked

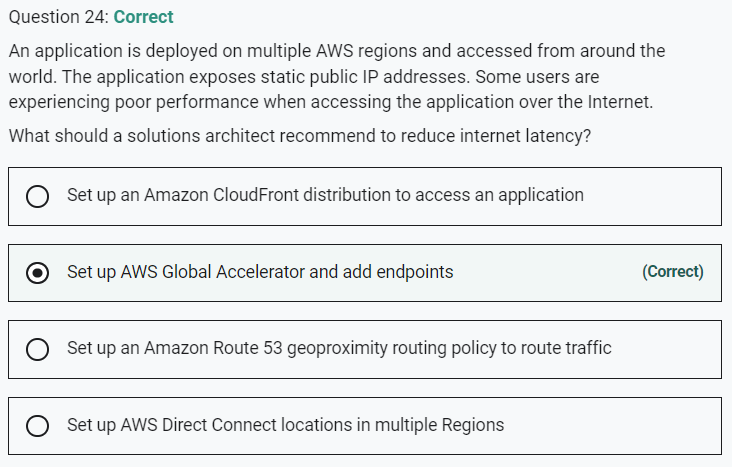




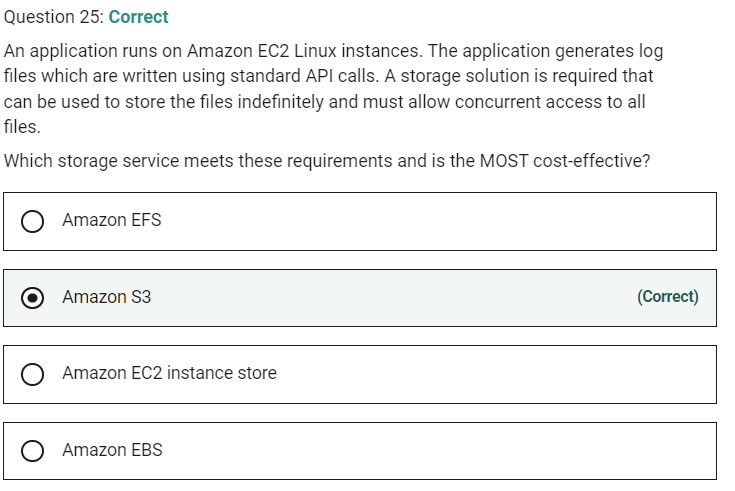


Marked

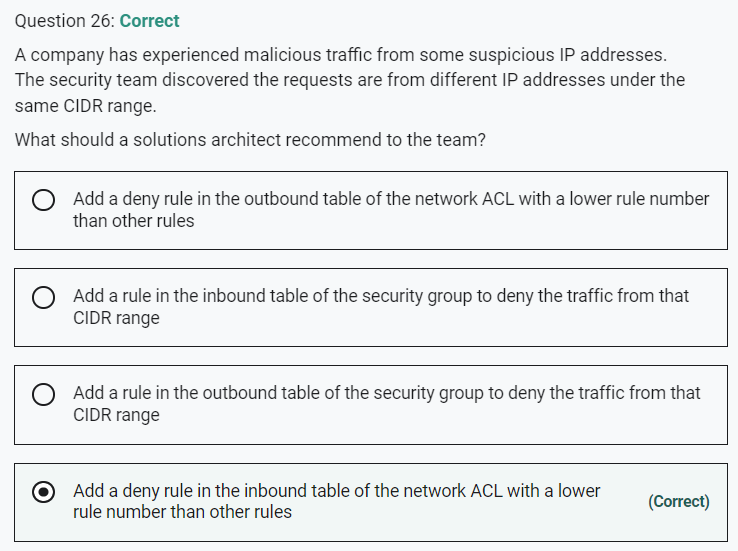




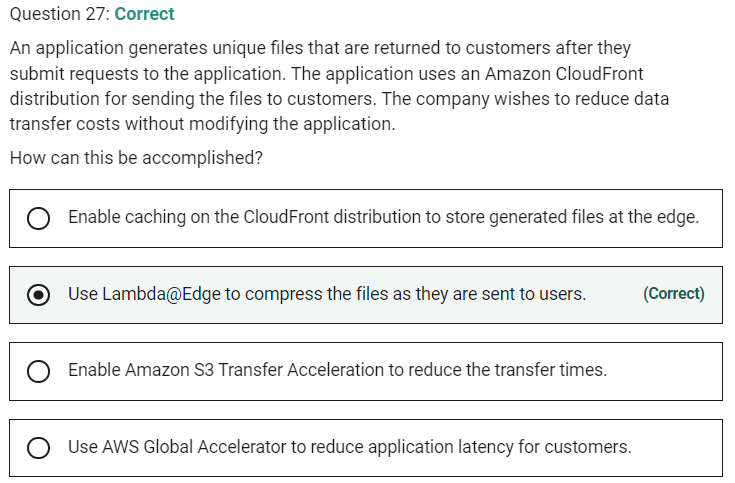
Marked



**INCORRECT:** "Amazon EFS" is incorrect as though this does offer concurrent access from many EC2 Linux instances, it is not the most cost-effective solution.

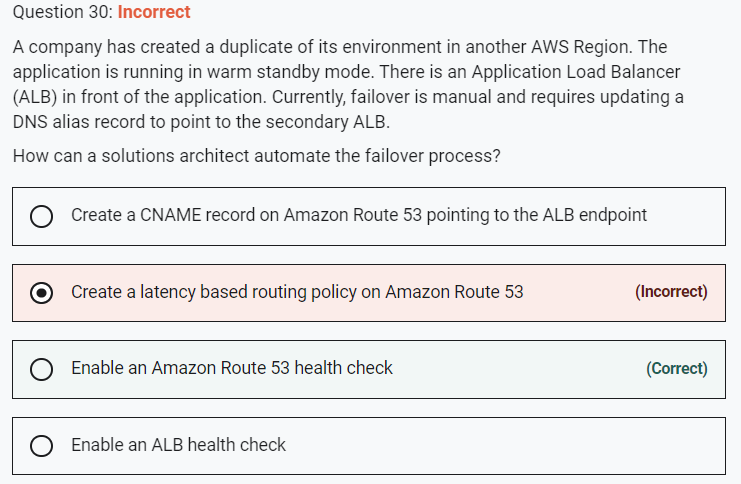


Marked





Marked



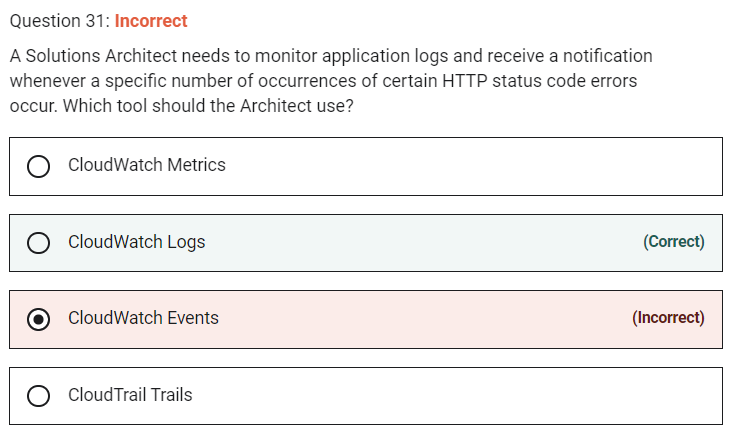
**CORRECT:**"Enable an Amazon Route 53 health check" is the correct answer.

**INCORRECT:** "Enable an ALB health check" is incorrect. The point of an ALB health check is to identify the health of targets (EC2 instances). It cannot redirect clients to another Region.

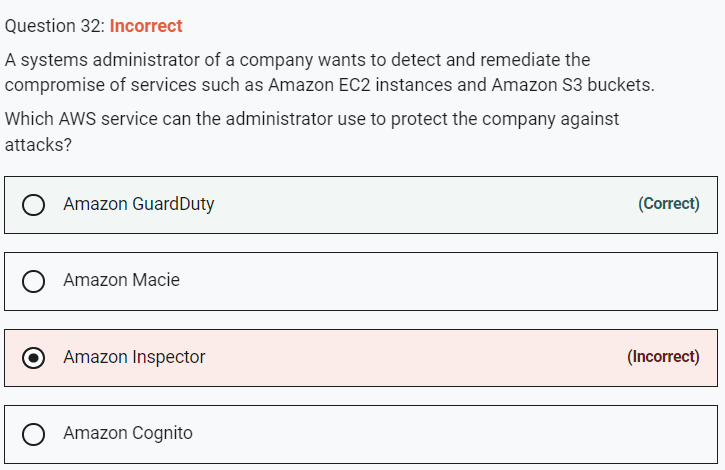
**INCORRECT:** "Create a CNAME record on Amazon Route 53 pointing to the ALB endpoint" is incorrect as an Alias record already exists and is better for mapping to an ALB.

**INCORRECT:** "Create a latency based routing policy on Amazon Route 53" is incorrect as this will only take into account latency, it is not used for failover.

Marked

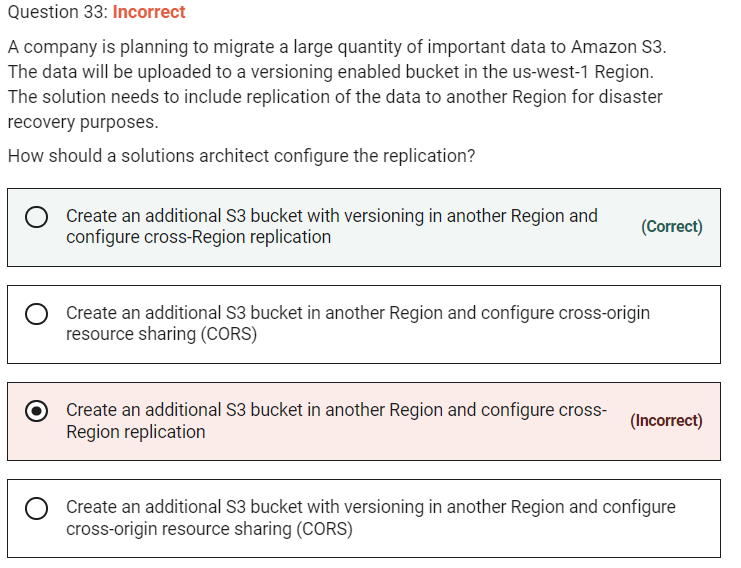


Marked

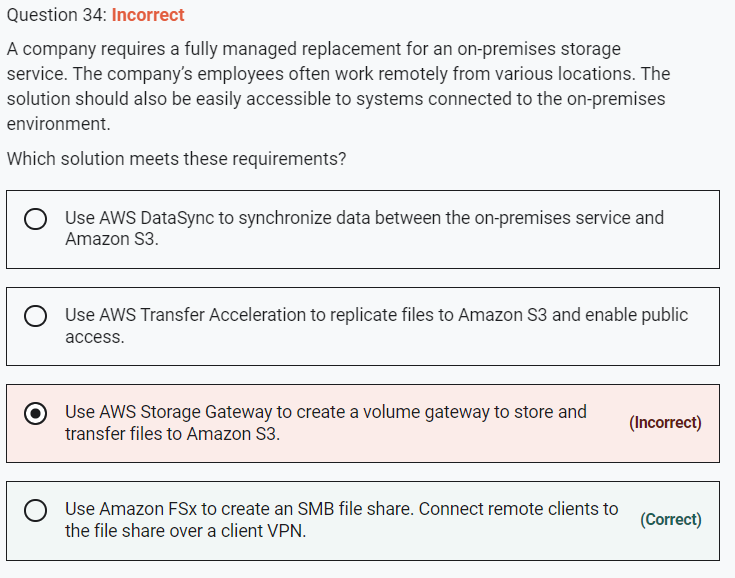


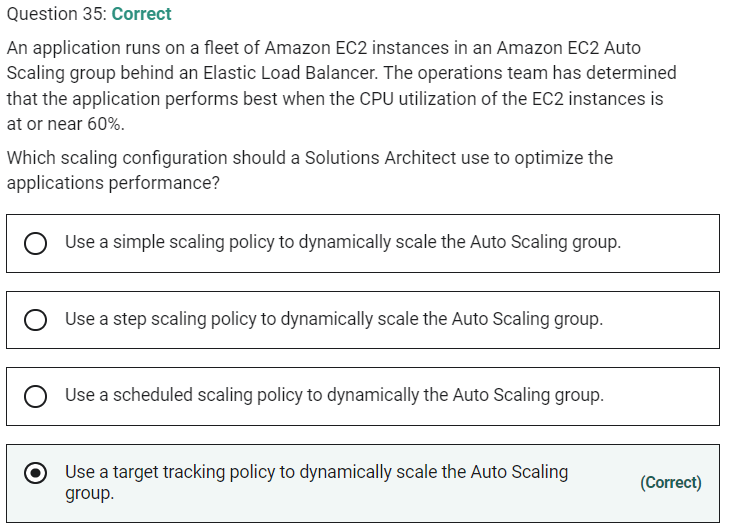
**INCORRECT:** "Amazon Inspector" is incorrect. Inspector is more about identifying vulnerabilities and evaluating against security best practices. It does not detect compromise.

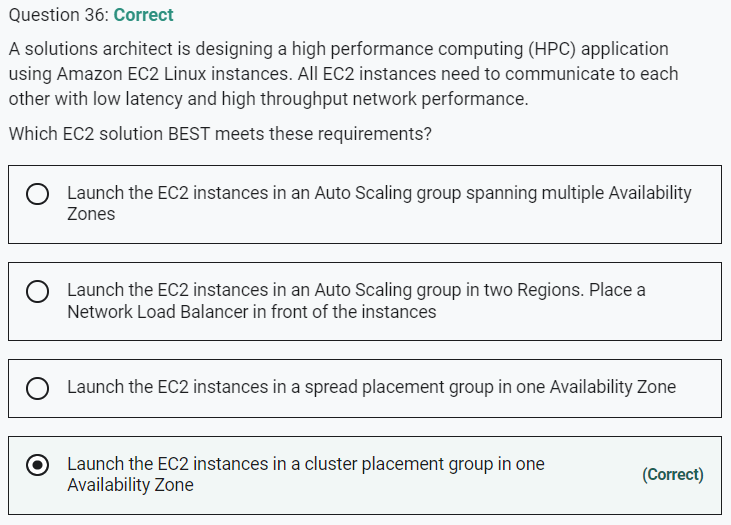
Marked

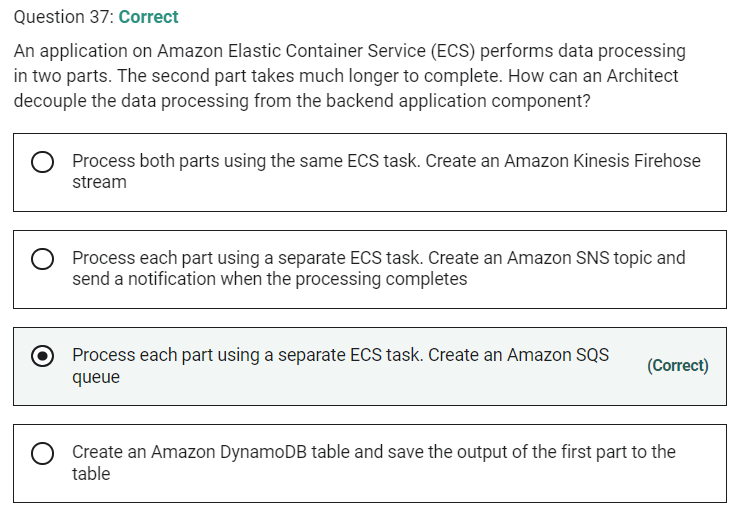


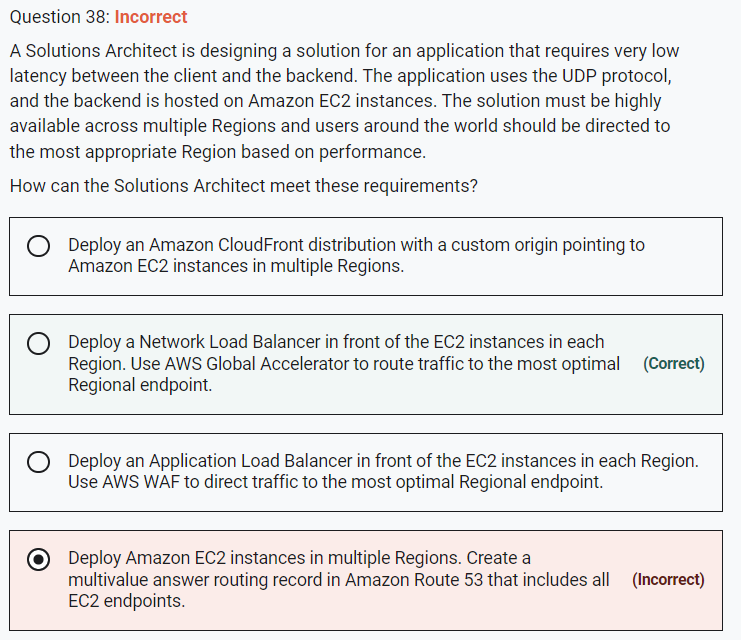
Marked

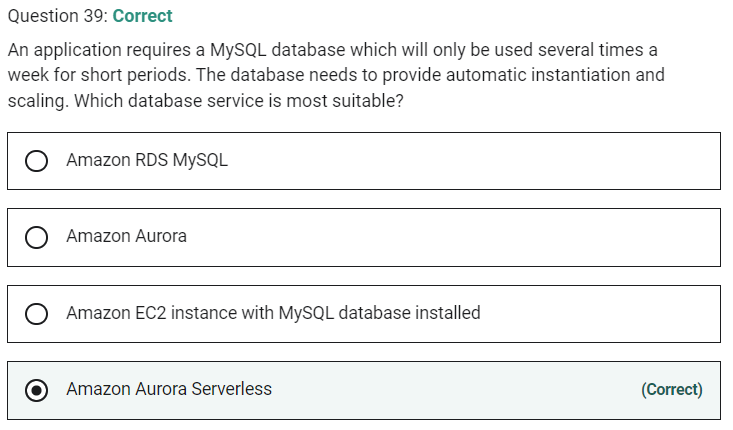




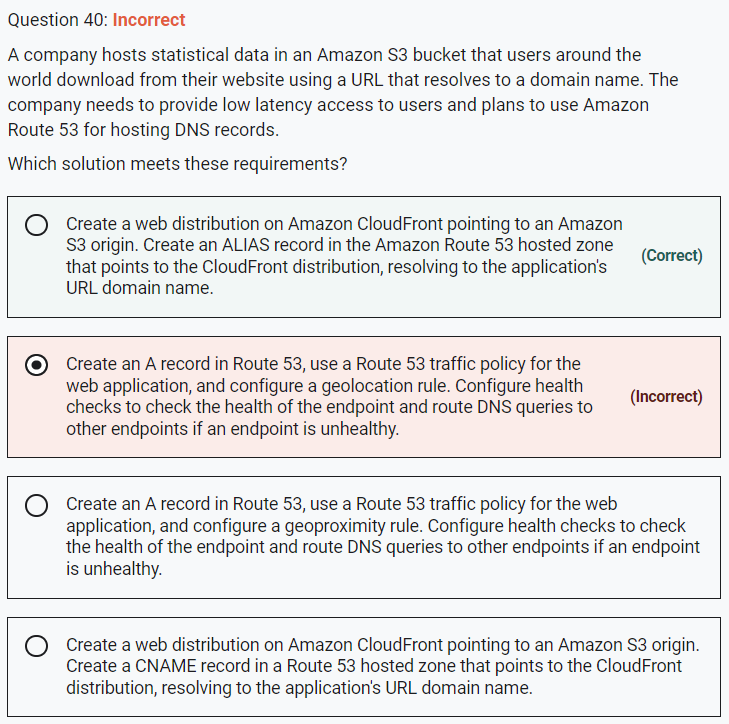








Marked



This is a simple requirement for low latency access to the contents of an Amazon S3 bucket for global users. The best solution here is to use Amazon CloudFront to cache the content in Edge Locations around the world. This involves creating a web distribution that points to an S3 origin (the bucket) and then create an Alias record in Route 53 that resolves the applications URL to the CloudFront distribution endpoint.

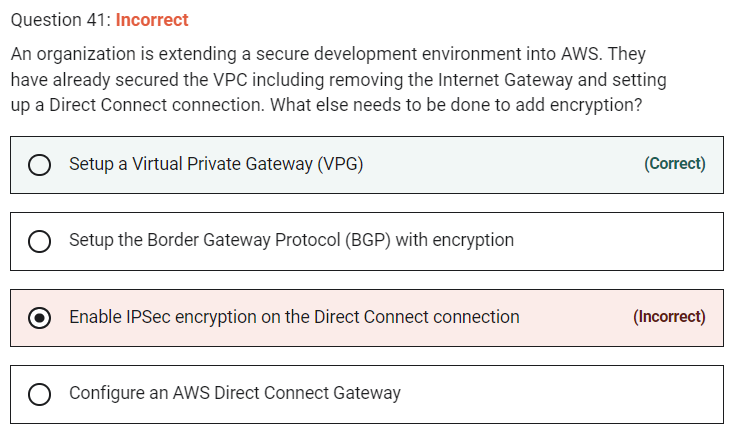
**CORRECT:**"Create a web distribution on Amazon CloudFront pointing to an Amazon S3 origin. Create an ALIAS record in the Amazon Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name" is the correct answer.

**INCORRECT:** "Create a web distribution on Amazon CloudFront pointing to an Amazon S3 origin. Create a CNAME record in a Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name" is incorrect. An Alias record should be used to point to an Amazon CloudFront distribution.

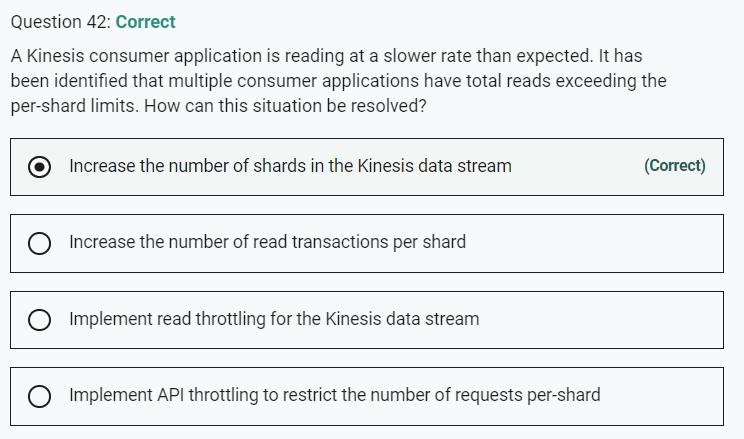
**INCORRECT:** "Create an A record in Route 53, use a Route 53 traffic policy for the web application, and configure a geolocation rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy" is incorrect. There is only a single endpoint (the Amazon S3 bucket) so this strategy would not work. Much better to use CloudFront to cache in multiple locations.

**INCORRECT:** "Create an A record in Route 53, use a Route 53 traffic policy for the web application, and configure a geoproximity rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy" is incorrect. Again, there is only one endpoint so this strategy will simply not work.

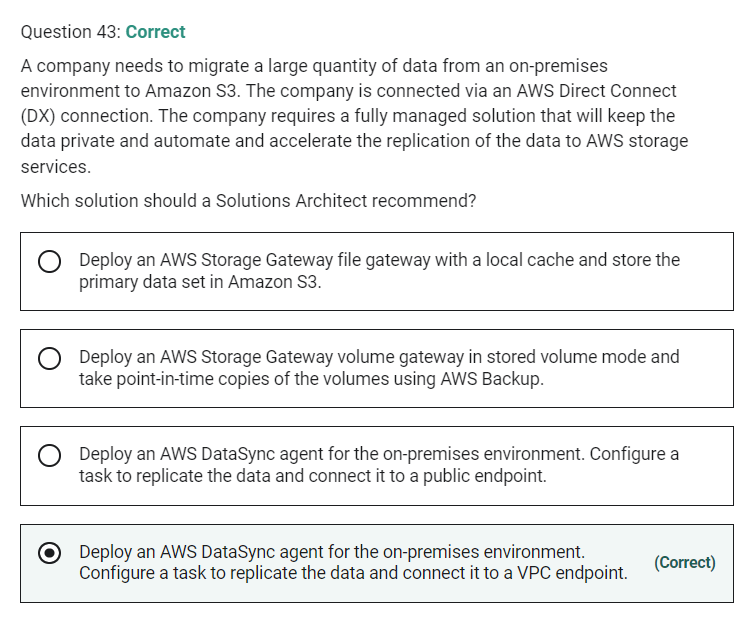
Marked



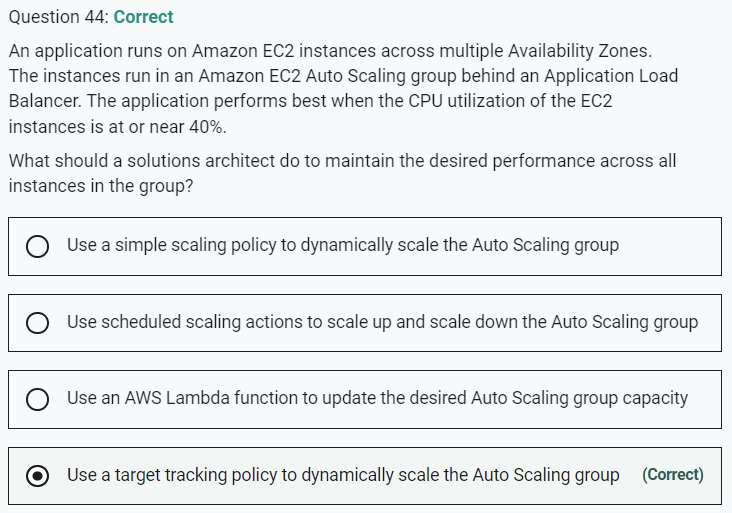
A VPG is used to setup an AWS VPN which you can use in combination with Direct Connect to encrypt all data that traverses the Direct Connect link.

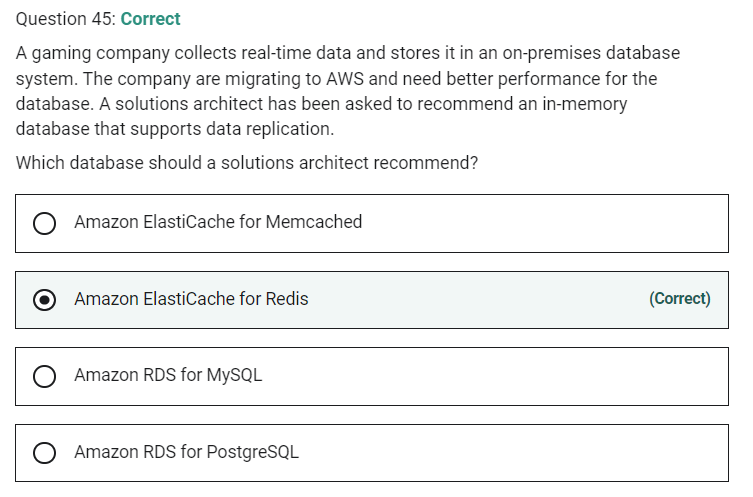


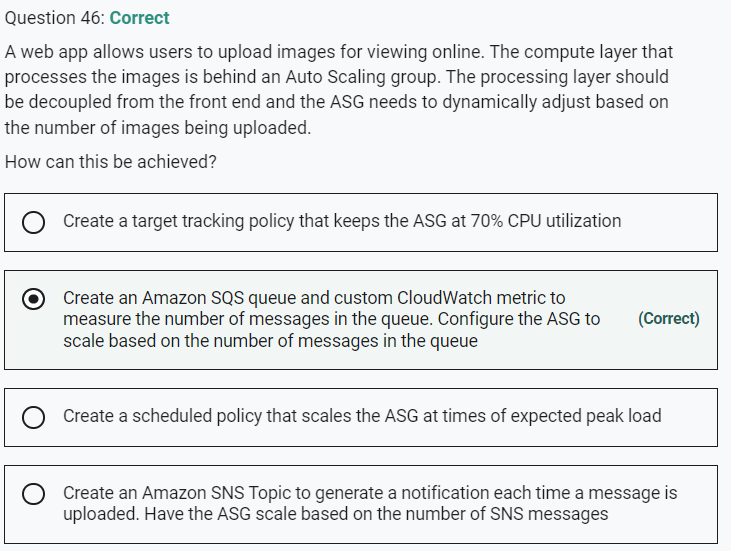
Marked

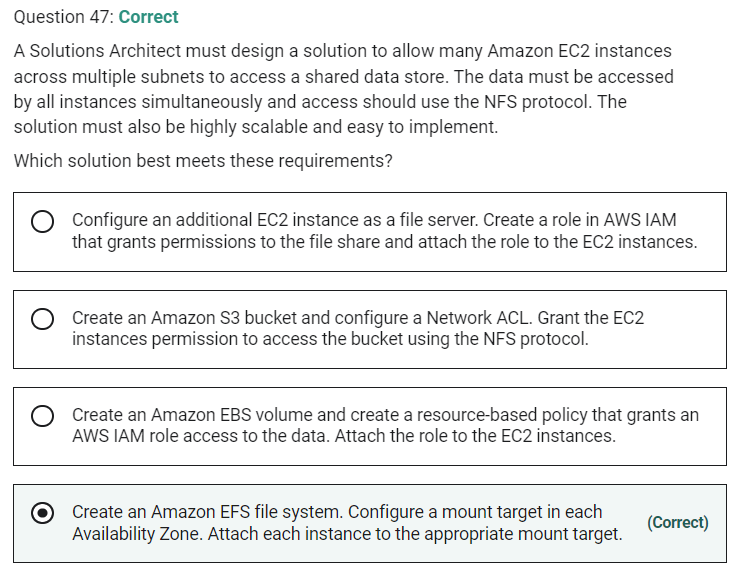


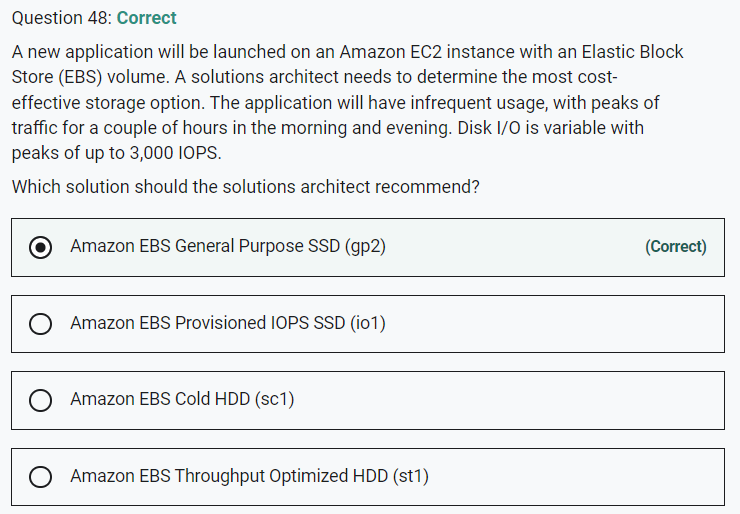
AWS DataSync can be used to automate and accelerate the replication of data to AWS storage services. Note that Storage Gateway is used for hybrid scenarios where servers need local access to data with various options for storing and synchronizing the data to AWS storage services. Storage Gateway does not accelerate replication of data.

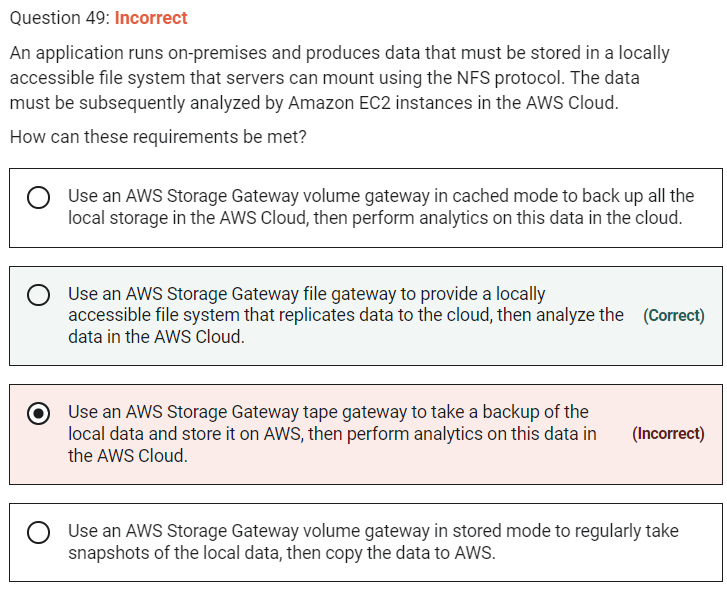




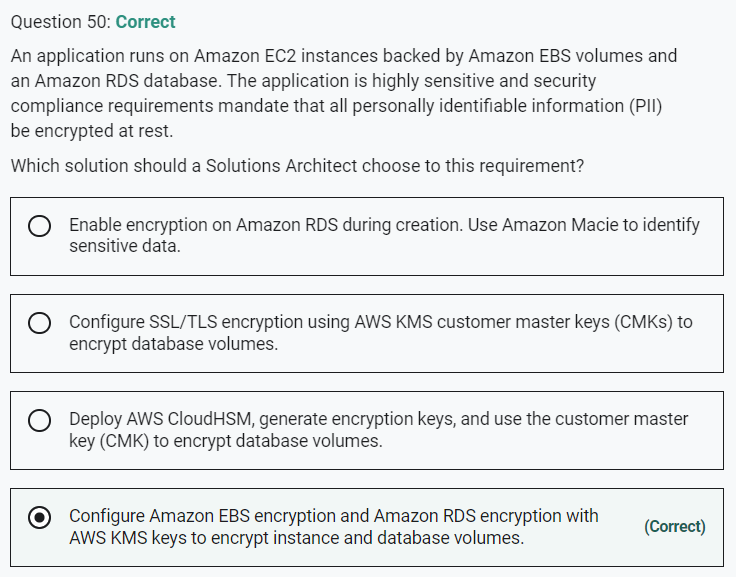




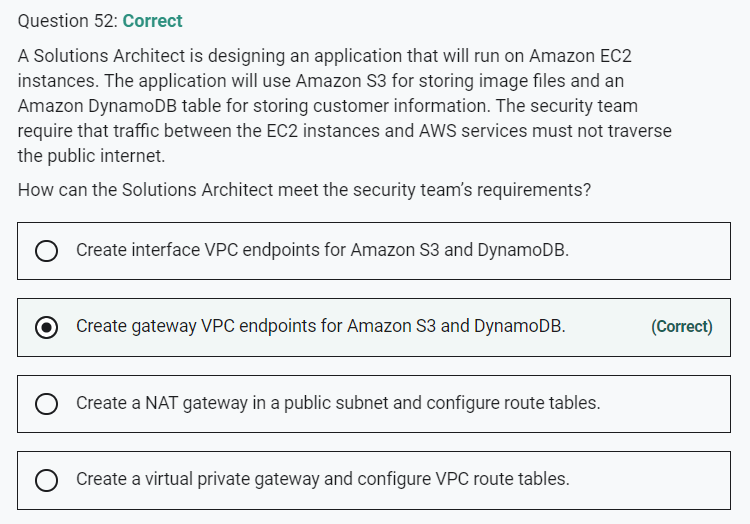


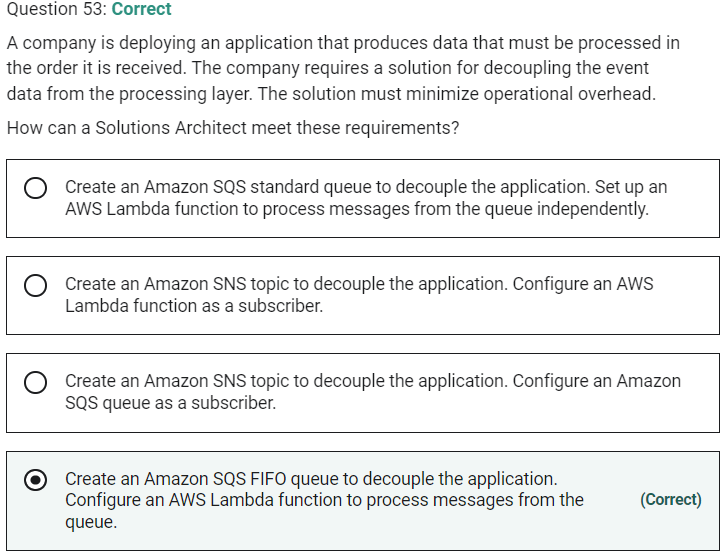


Marked

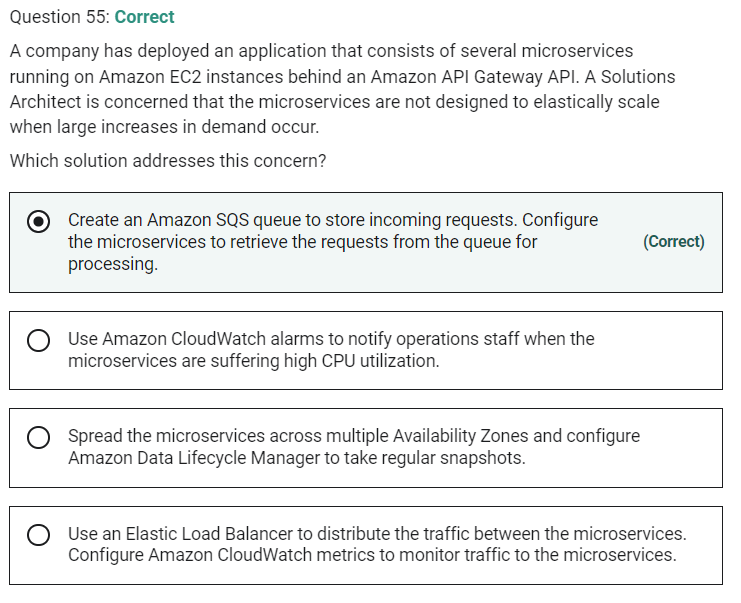




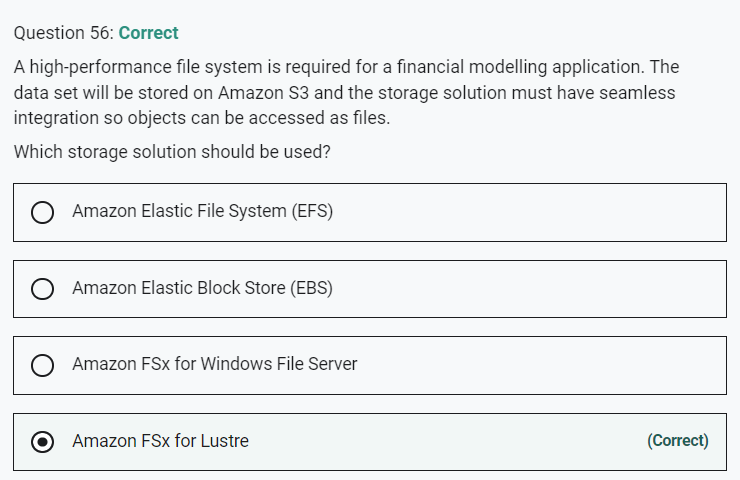




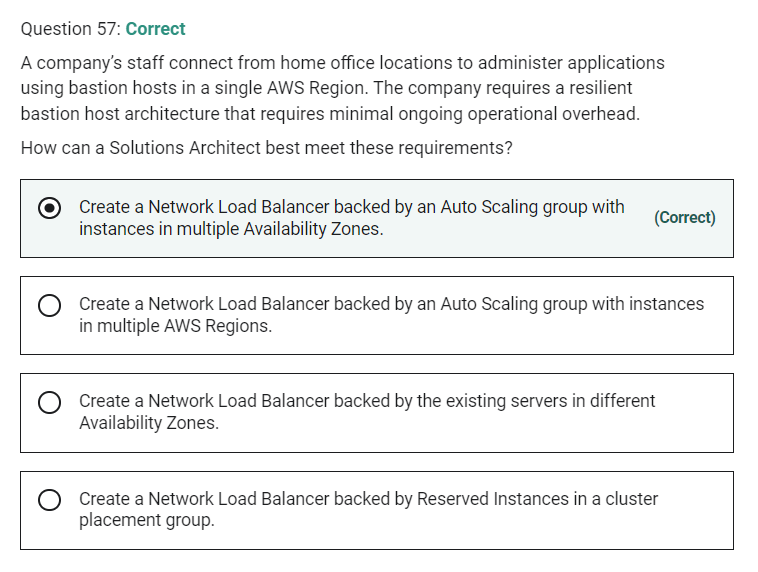




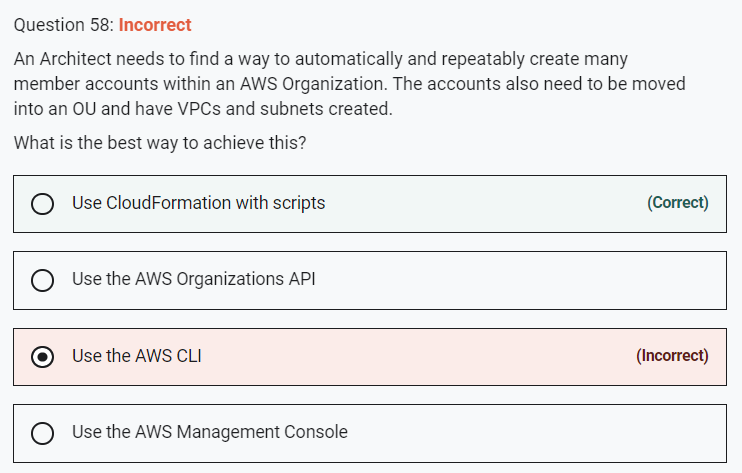
Marked

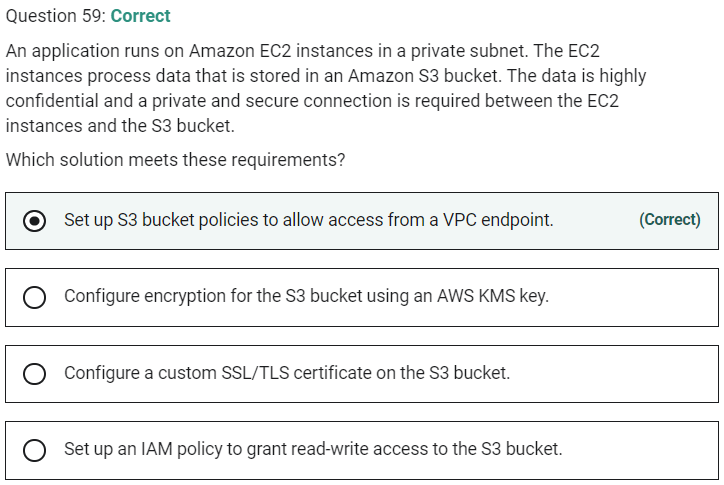


Marked

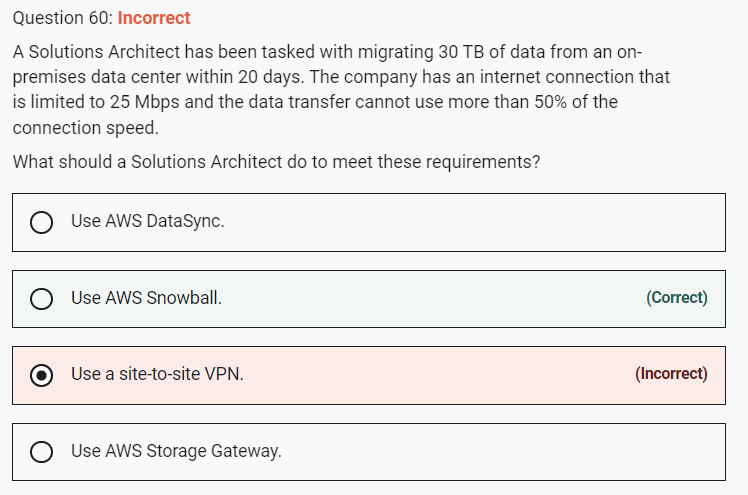


Marked





Marked



This is a simple case of working out roughly how long it will take to migrate the data using the 12.5 Mbps of bandwidth that is available for transfer and seeing which options are feasible. Transferring 30 TB of data across a 25 Mbps connection could take upwards of 200 days.

Therefore, we know that using the Internet connection will not meet the requirements and we can rule out any solution that will use the internet (all options except for Snowball). AWS Snowball is a physical device that is shipped to your office or data center. You can then load data onto it and ship it back to AWS where the data is uploaded to Amazon S3.

Snowball is the only solution that will achieve the data migration requirements within the 20-day period.

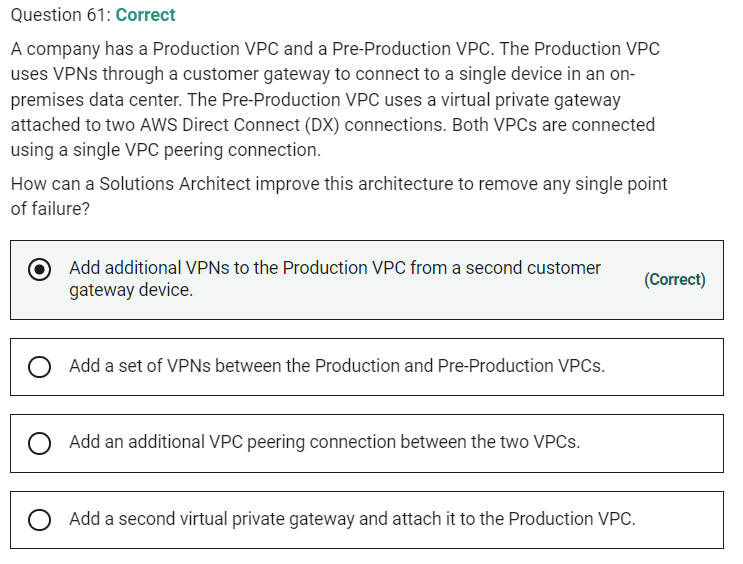
**CORRECT:**"Use AWS Snowball" is the correct answer.

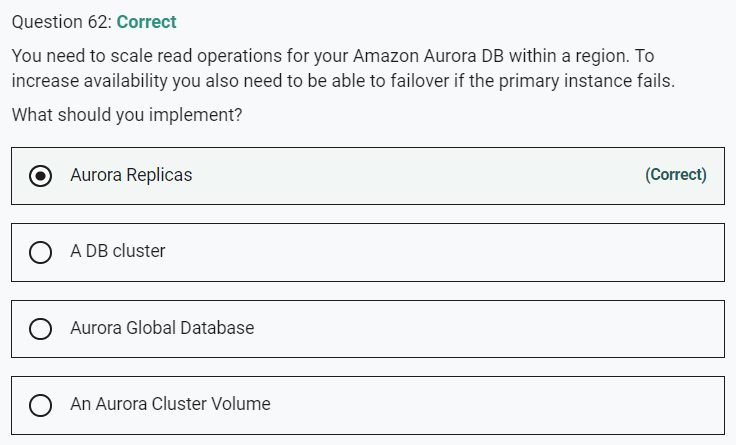
**INCORRECT:** "Use AWS DataSync" is incorrect. This uses the internet which will not meet the 20-day deadline.

**INCORRECT:** "Use AWS Storage Gateway" is incorrect. This uses the internet which will not meet the 20-day deadline.

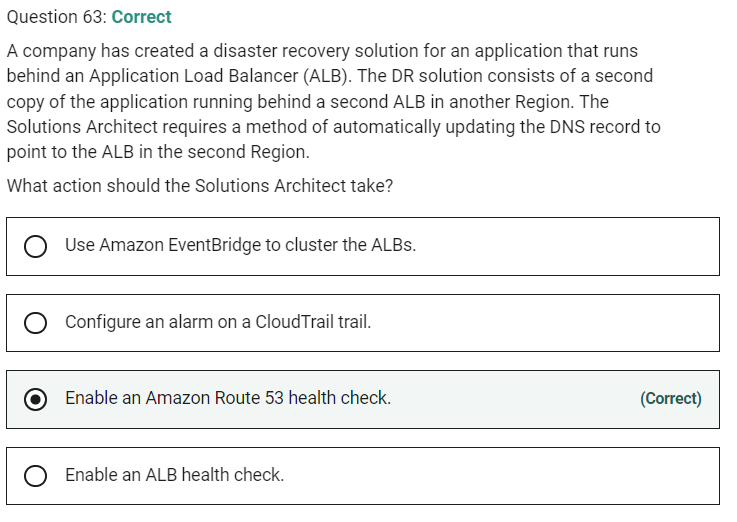
**INCORRECT:** "Use a site-to-site VPN" is incorrect. This uses the internet which will not meet the 20-day deadline.

Marked





Marked



Marked



Marked

