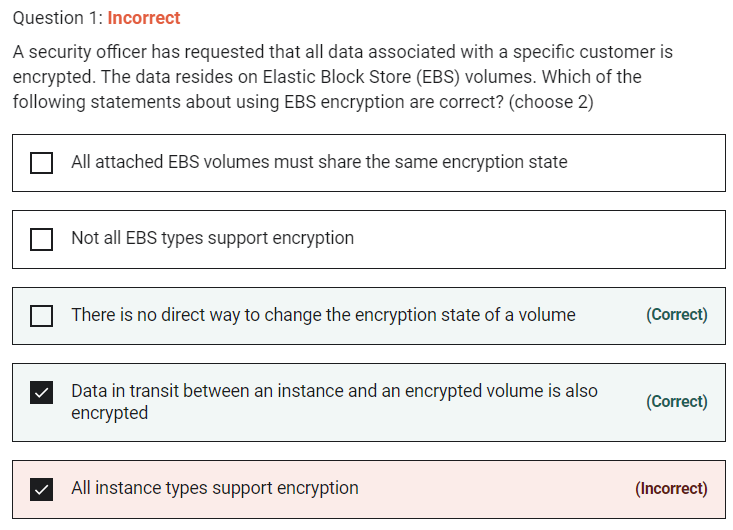
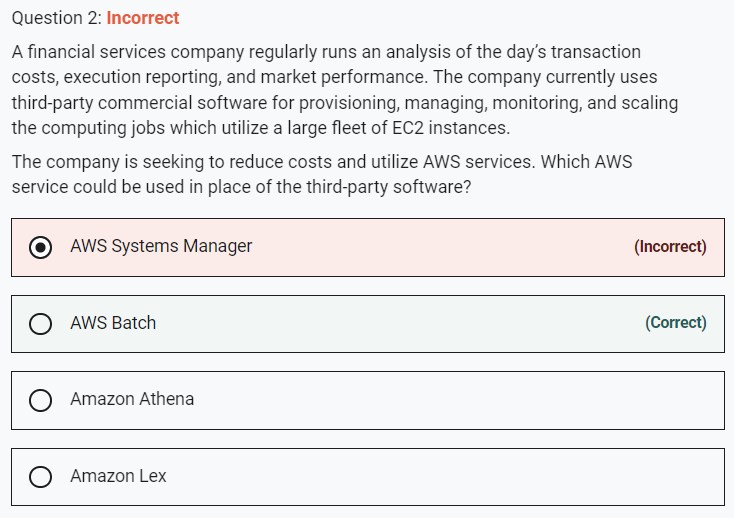
Marked



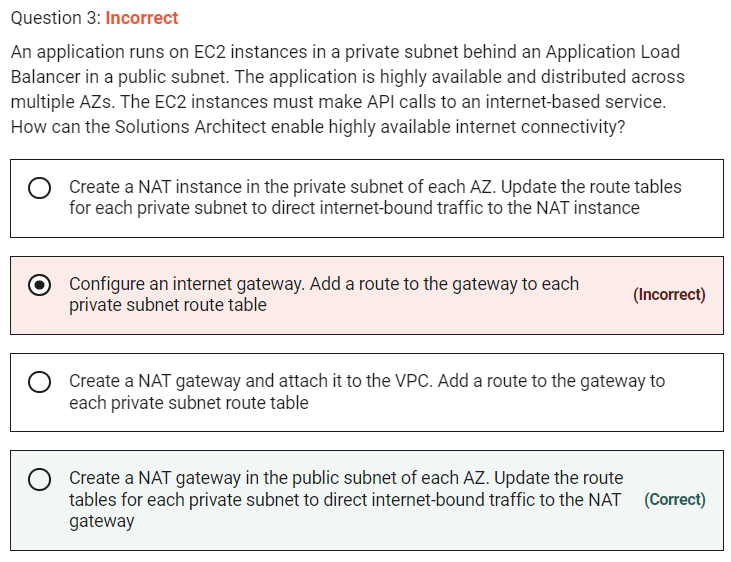
All EBS types and all instance families support encryption but not all instance types support encryption. There is no direct way to change the encryption state of a volume. Data in transit between an instance and an encrypted volume is also encrypted.

Marked

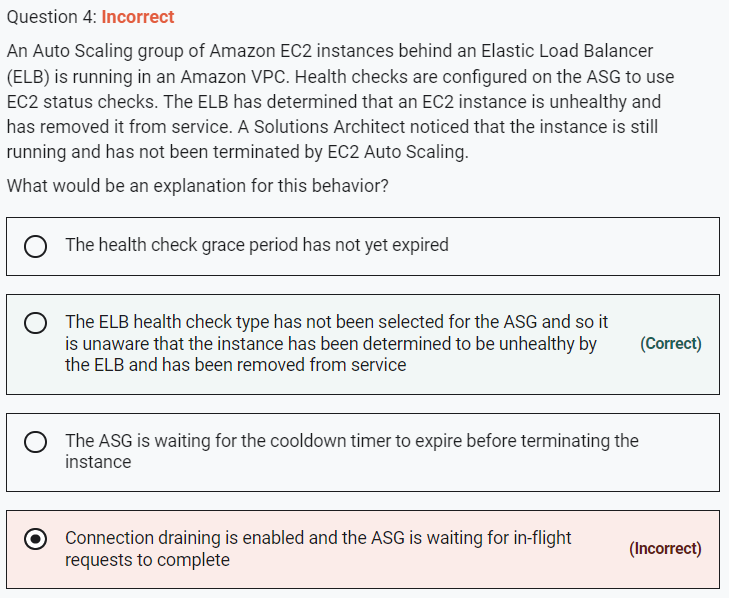


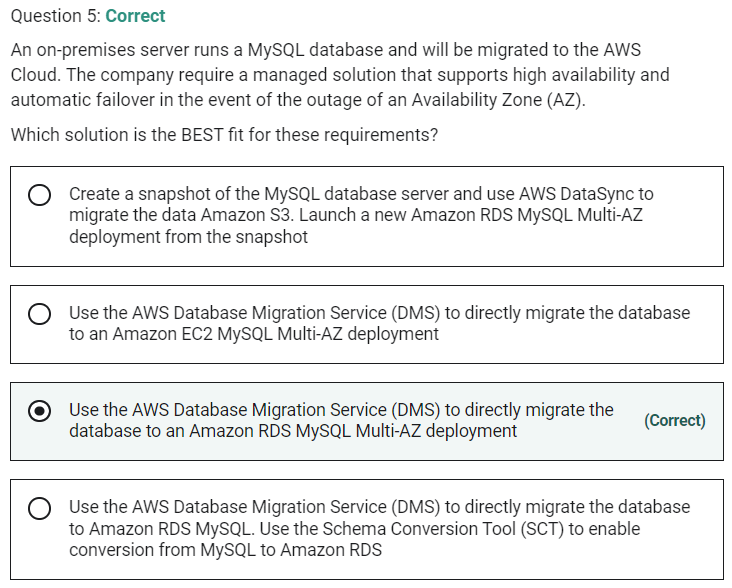
AWS Batch eliminates the need to operate third-party commercial or open source batch processing solutions.

Marked

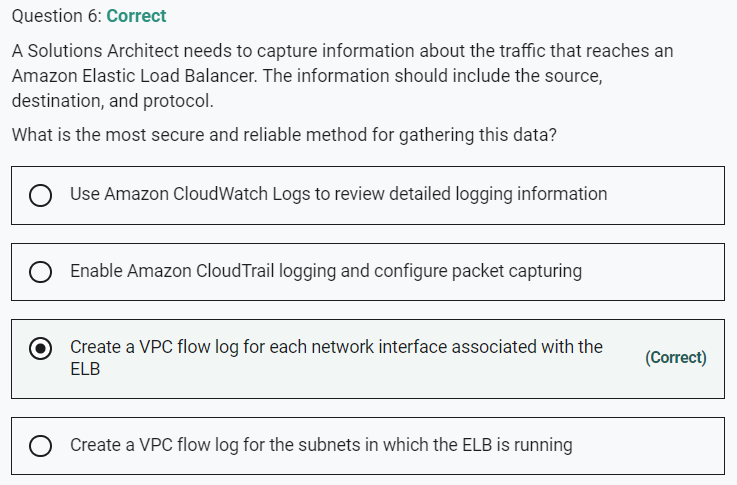


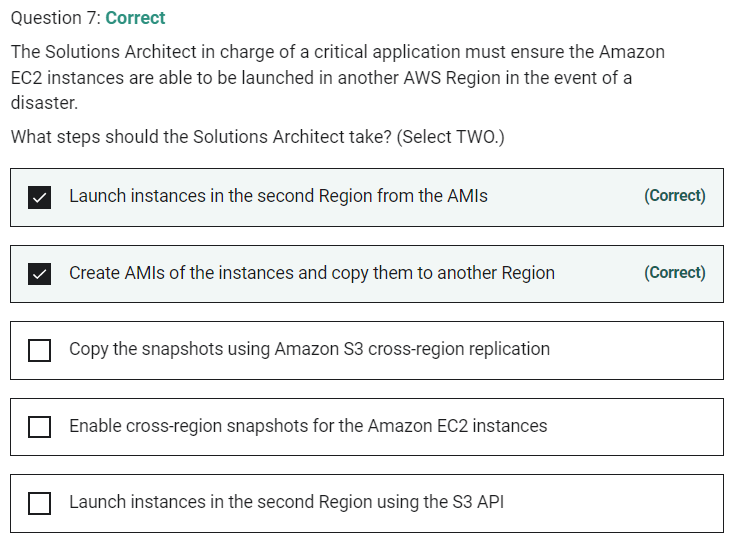
Marked

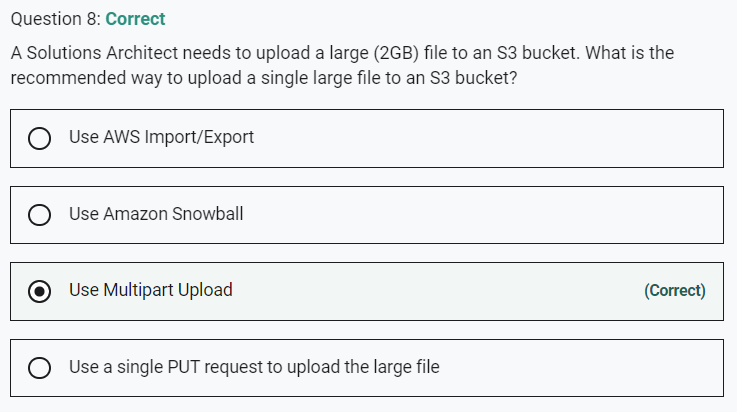


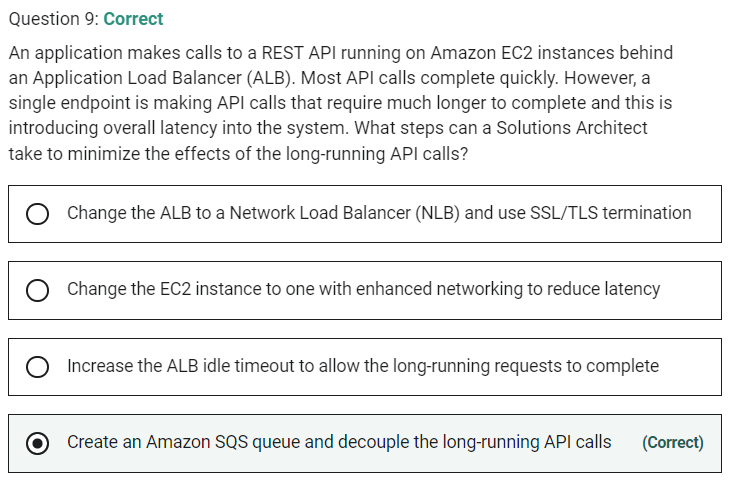


Marked

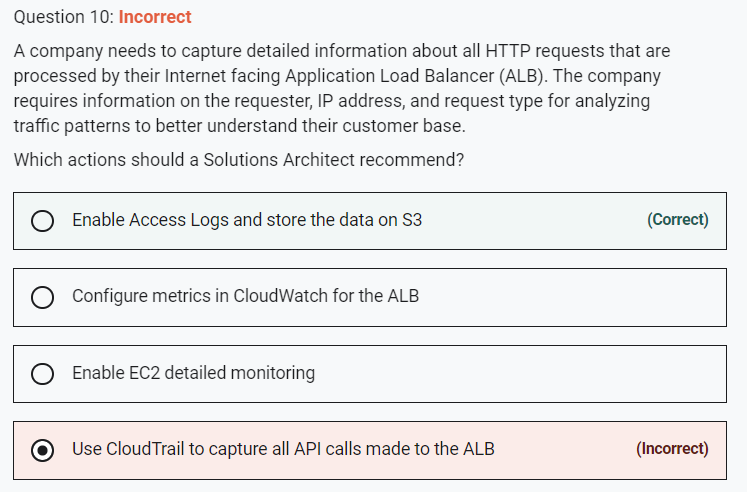




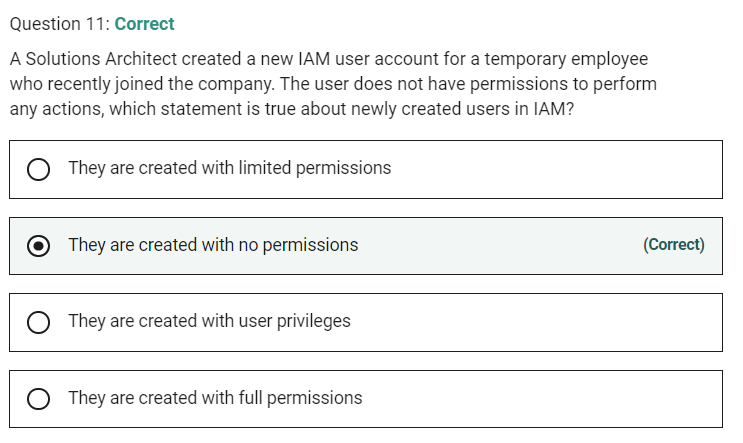




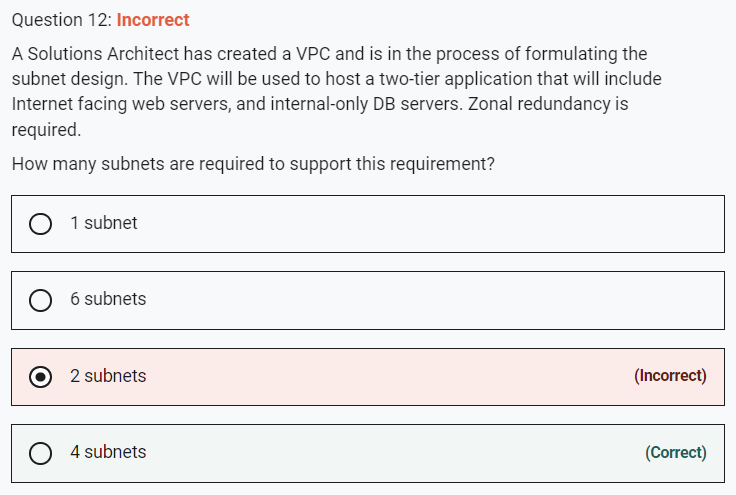
Marked



**INCORRECT:** Use CloudTrail to capture all API calls made to the ALB"" is incorrect. CloudTrail captures API activity and would not include the requested information.



Marked



**Explanation**

Zonal redundancy indicates that the architecture should be split across multiple Availability Zones. Subnets are mapped 1:1 to AZs.

A public subnet should be used for the Internet-facing web servers and a separate private subnet should be used for the internal-only DB servers. Therefore you need 4 subnets – 2 (for redundancy) per public/private subnet.

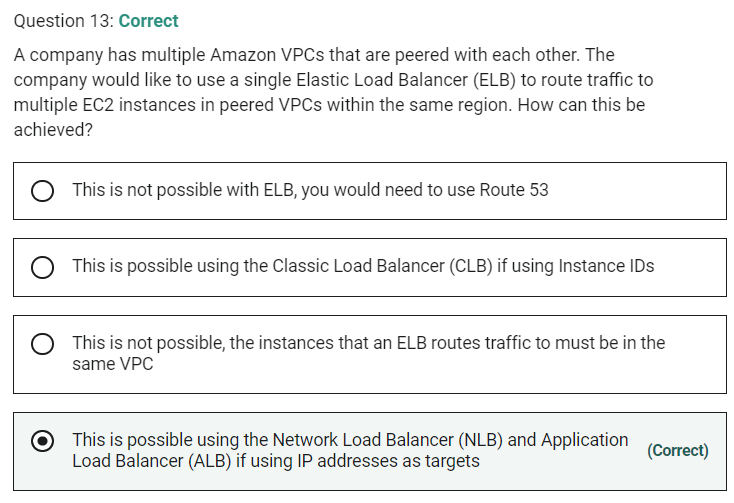
**CORRECT:**"4 subnets" is the correct answer.

**INCORRECT:** "2 subnets" is incorrect as explained above.

**INCORRECT:** "6 subnets" is incorrect as explained above.

**INCORRECT:** "2 subnet" is incorrect as explained above.

Marked

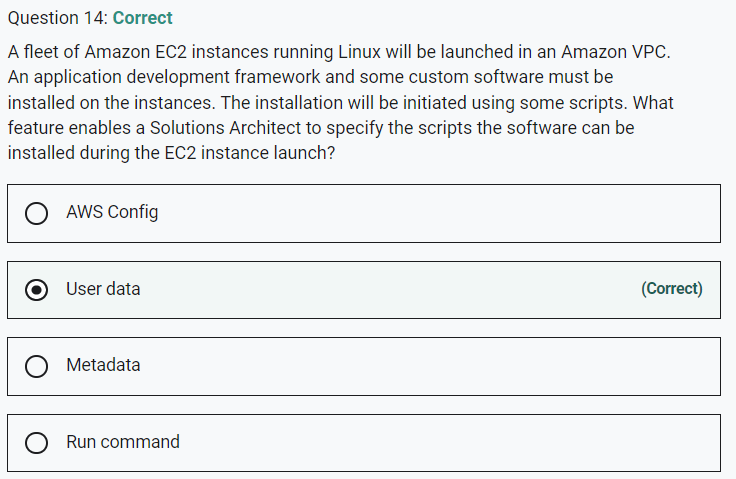


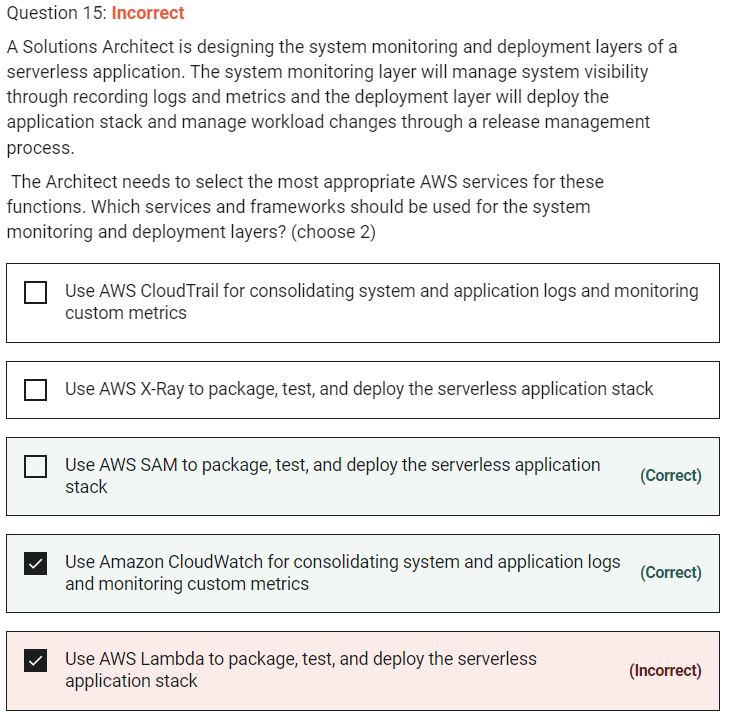
With ALB and NLB IP addresses can be used to register:

- Instances in a peered VPC.

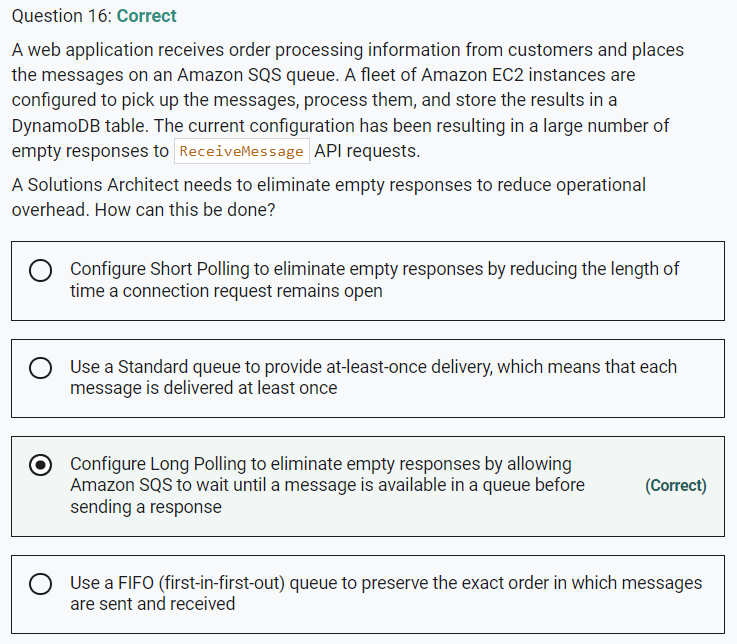
- AWS resources that are addressable by IP address and port.

- On-premises resources linked to AWS through Direct Connect or a VPN connection.

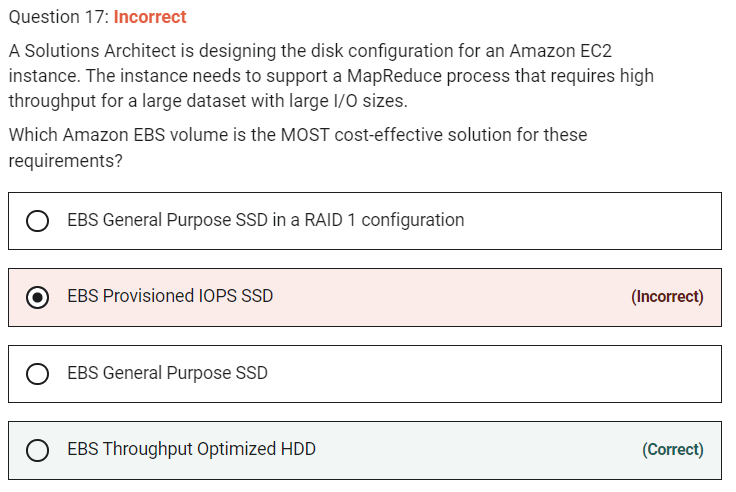




AWS Serverless Application Model (AWS SAM) is an extension of AWS CloudFormation that is used to package, test, and deploy serverless applications.



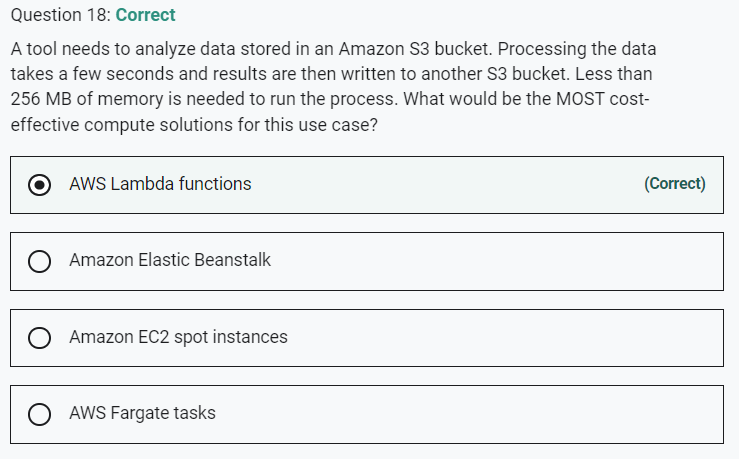
Marked

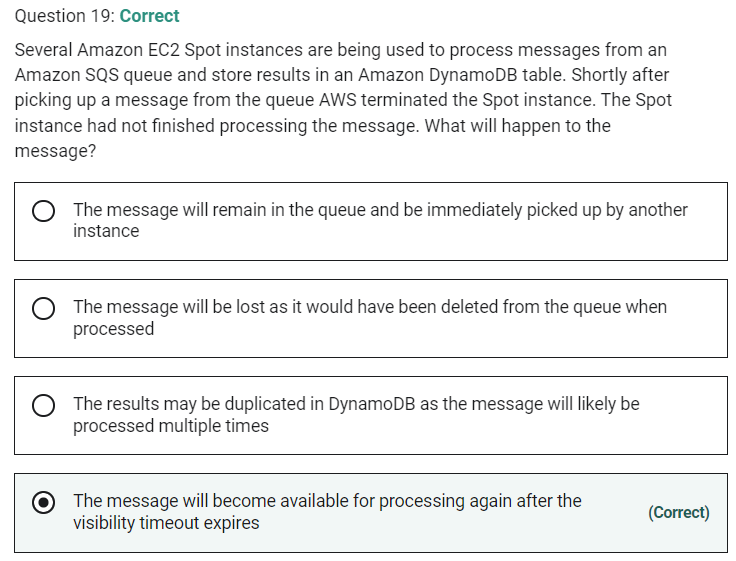


EBS Throughput Optimized HDD is good for the following use cases (and is the most cost-effective option:

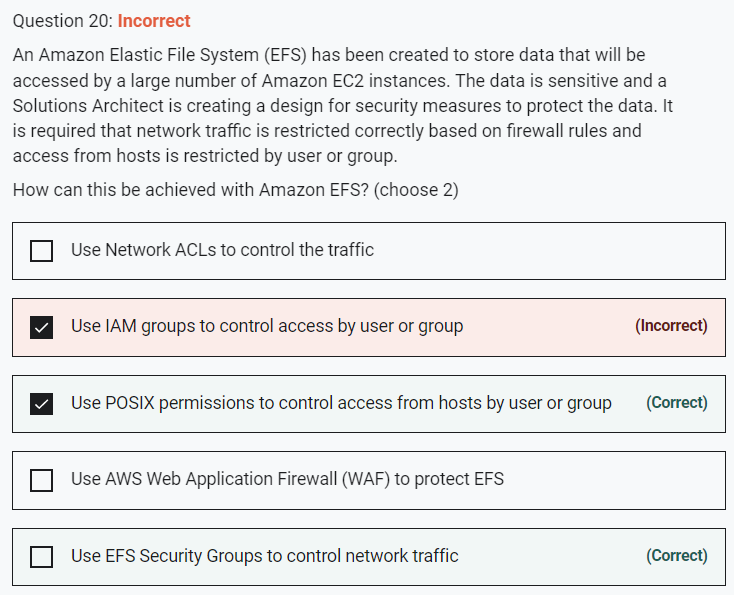
- Frequently accessed, throughput intensive workloads with large datasets and large I/O sizes, such as MapReduce, Kafka, log processing, data warehouse, and ETL workloads.

Throughput is measured in MB/s, and includes the ability to burst up to 250 MB/s per TB, with a baseline throughput of 40 MB/s per TB and a maximum throughput of 500 MB/s per volume.

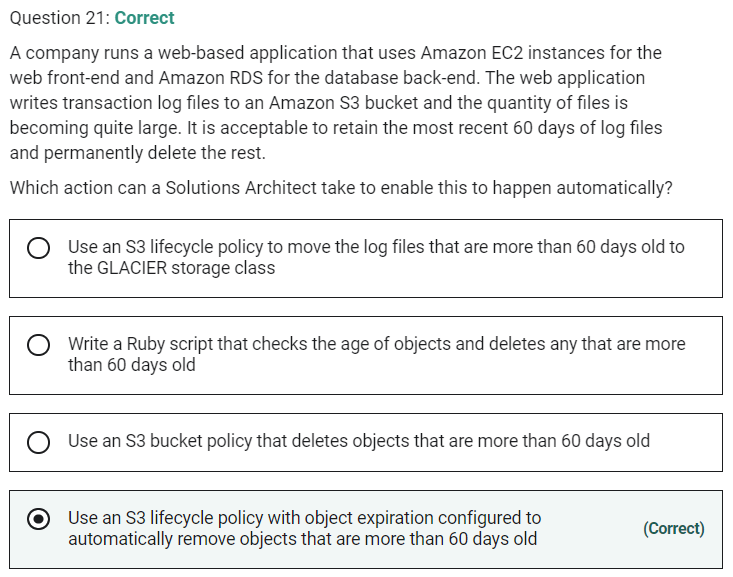


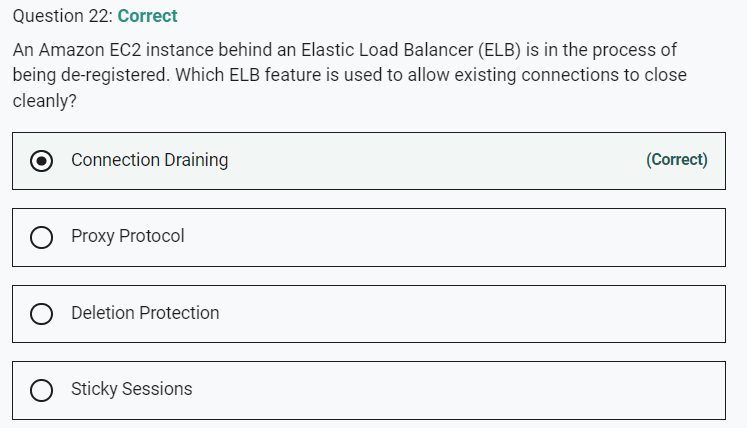


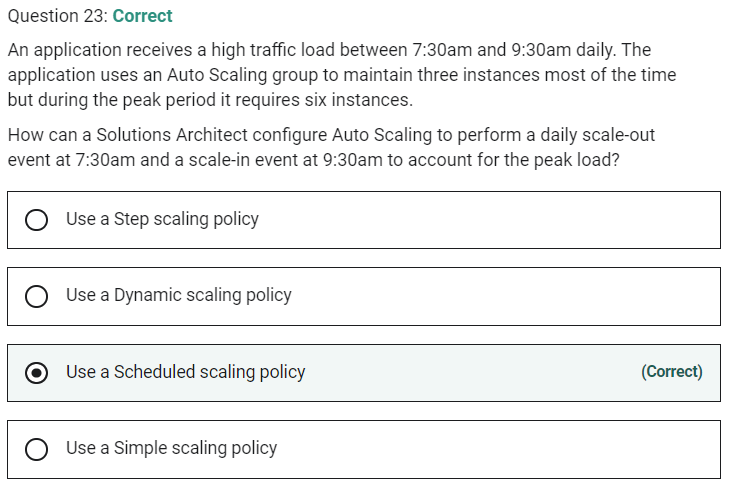
Marked



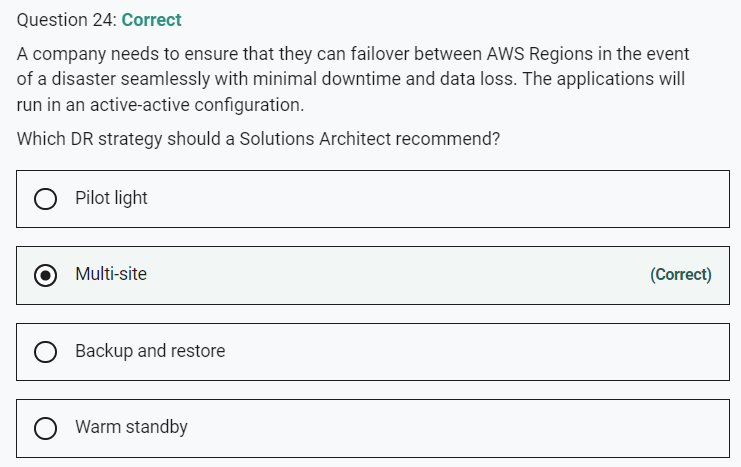
You can control who can administer your file system using IAM. You can control access to files and directories with POSIX-compliant user and group-level permissions. POSIX permissions allows you to restrict access from hosts by user and group. EFS Security Groups act as a firewall, and the rules you add define the traffic flow.

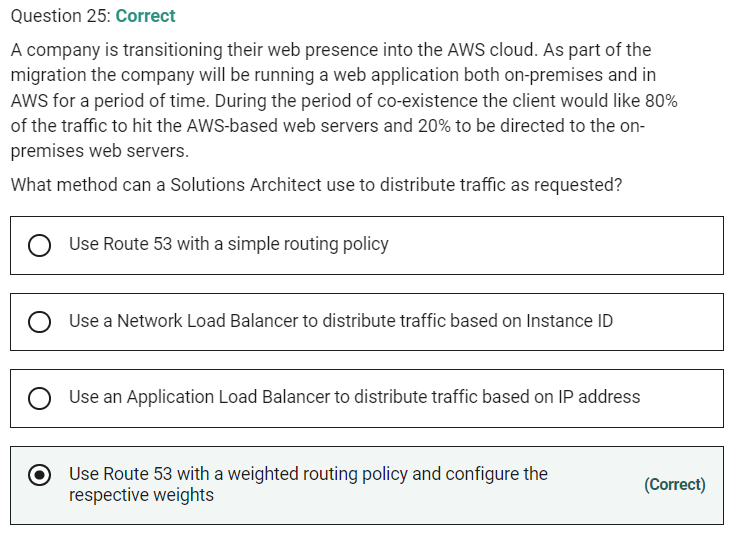


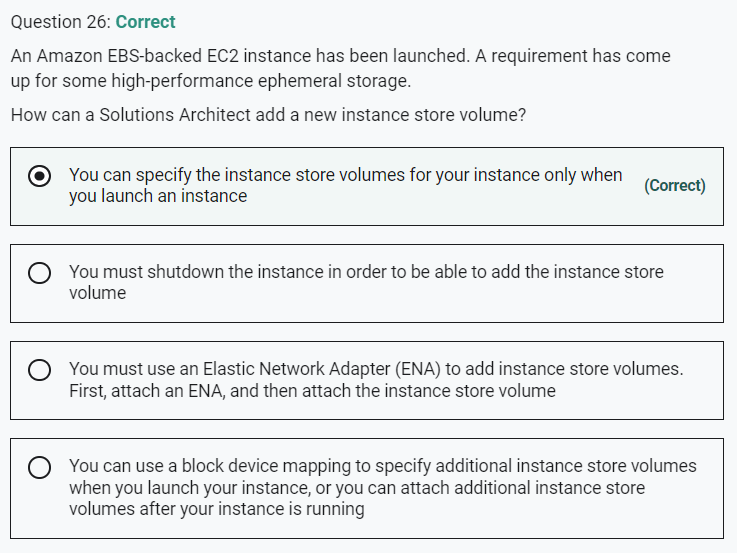


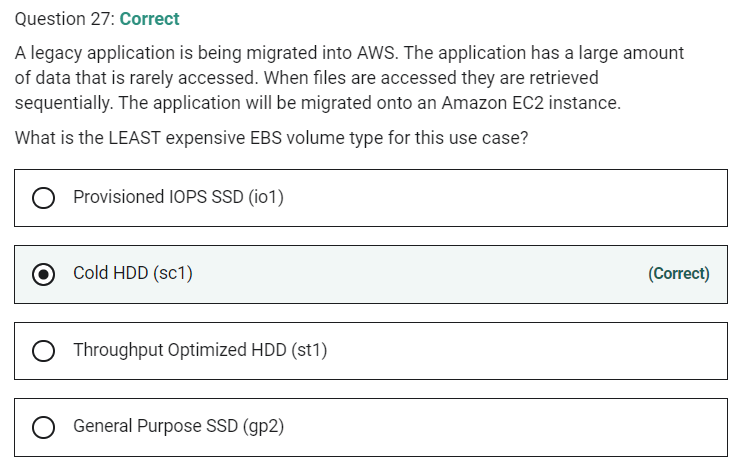


Marked

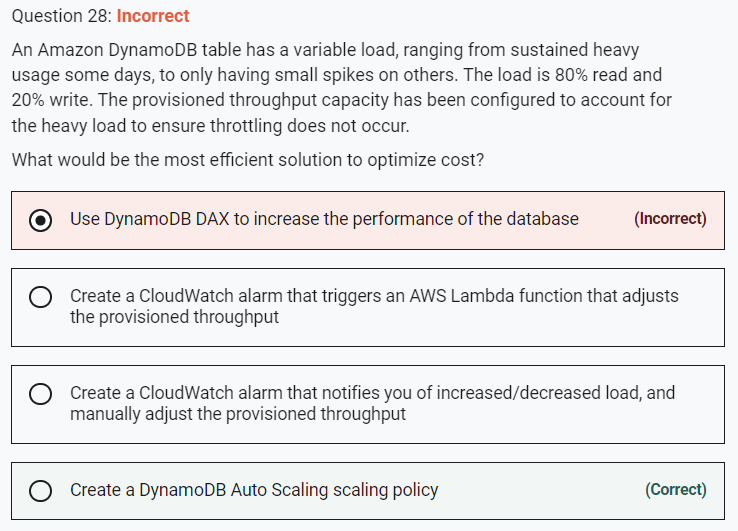








Marked



Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns. This is the most efficient and cost-effective solution to optimizing for cost.

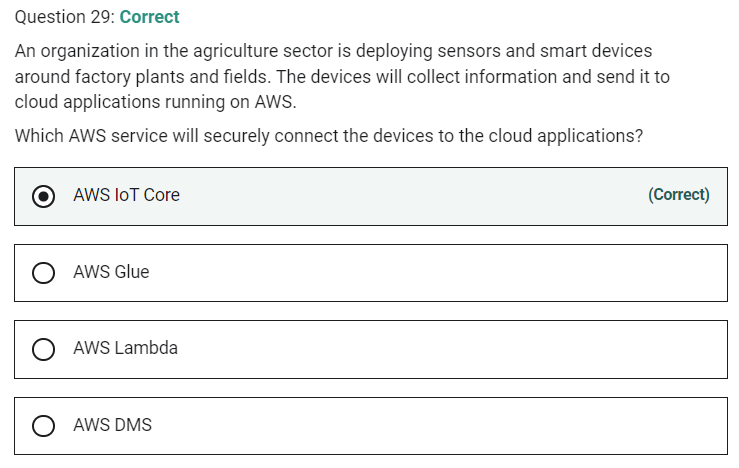
**CORRECT:**"Create a DynamoDB Auto Scaling scaling policy" is the correct answer.

**INCORRECT:** "Create a CloudWatch alarm that triggers an AWS Lambda function that adjusts the provisioned throughput" is incorrect. Using AWS Lambda to modify the provisioned throughput is possible but it would be more cost-effective to use DynamoDB Auto Scaling as there is no cost to using it.

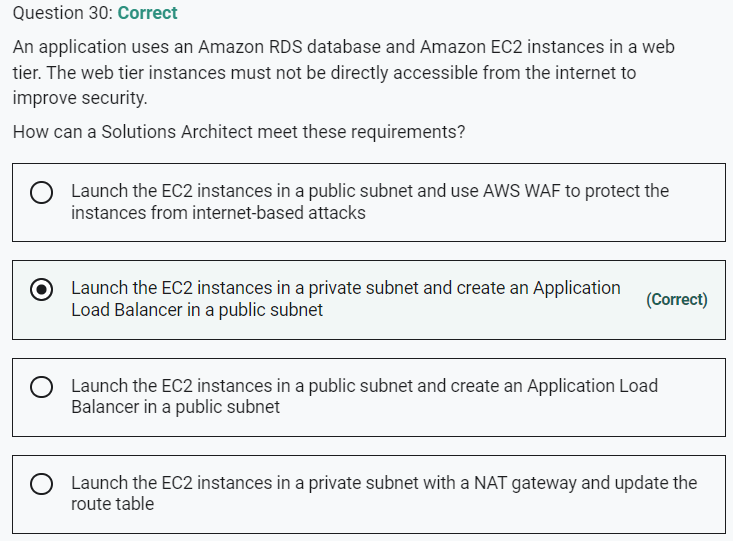
**INCORRECT:** "Create a CloudWatch alarm that notifies you of increased/decreased load, and manually adjust the provisioned throughput" is incorrect. Manually adjusting the provisioned throughput is not efficient.

**INCORRECT:** "Use DynamoDB DAX to increase the performance of the database" is incorrect. DynamoDB DAX is an in-memory cache that increases the performance of DynamoDB. However, it costs money and there is no requirement to increase performance.

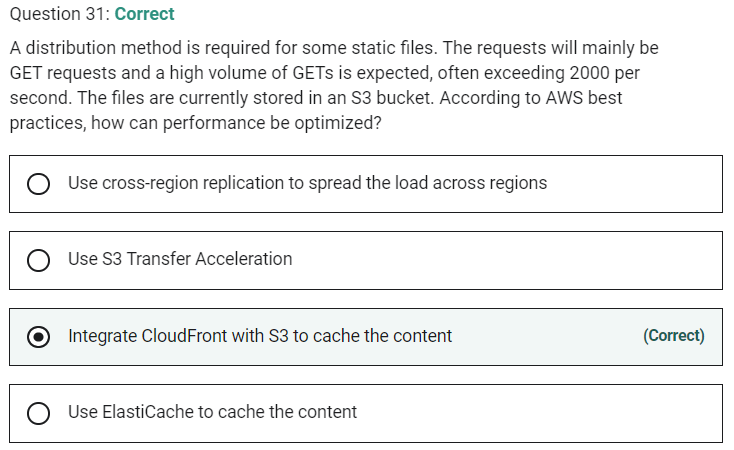
Marked



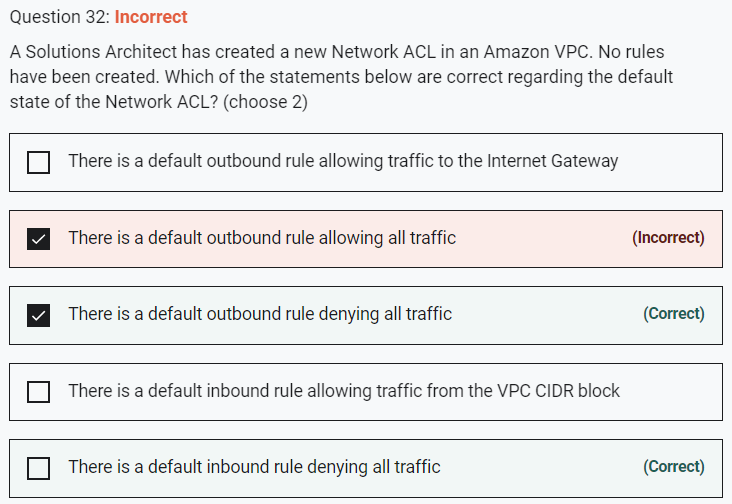
Marked



To prevent direct connectivity to the EC2 instances from the internet you can deploy your EC2 instances in a private subnet and have the ELB in a public subnet. To configure this you must enable a public subnet in the ELB that is in the same AZ as the private subnet.

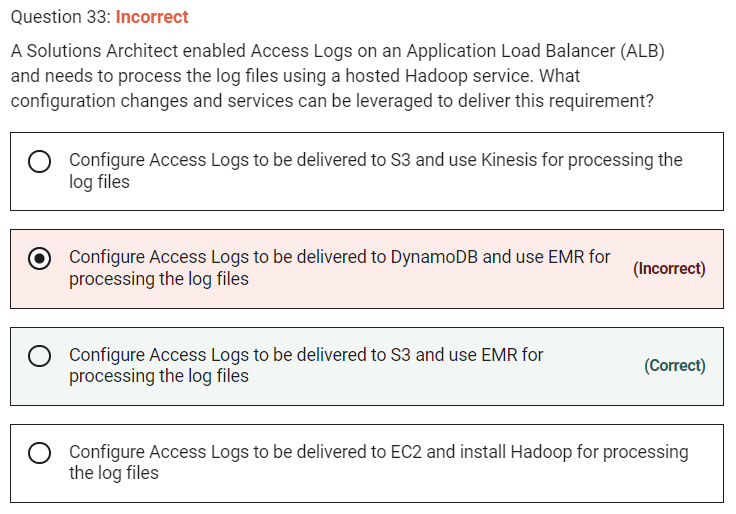


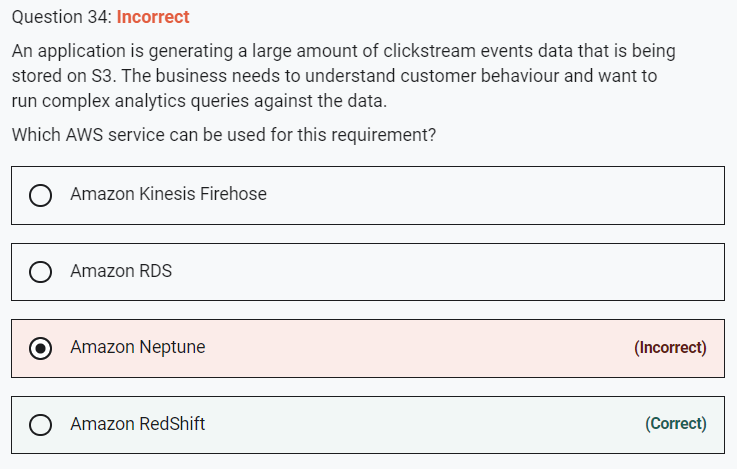
Marked



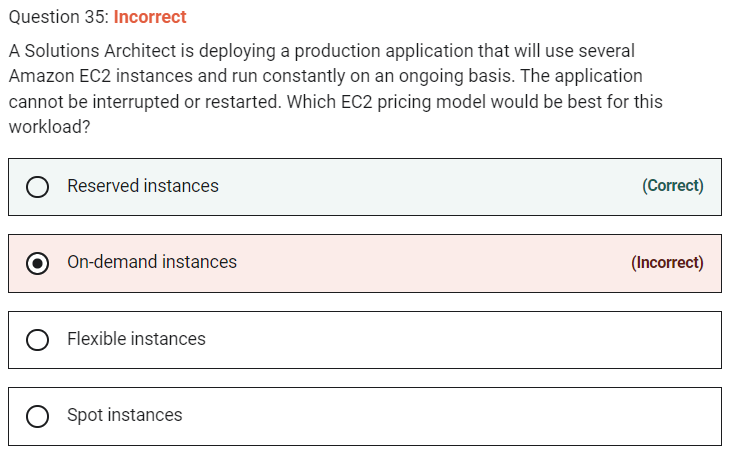
This is custom NACL that denies everything

Marked

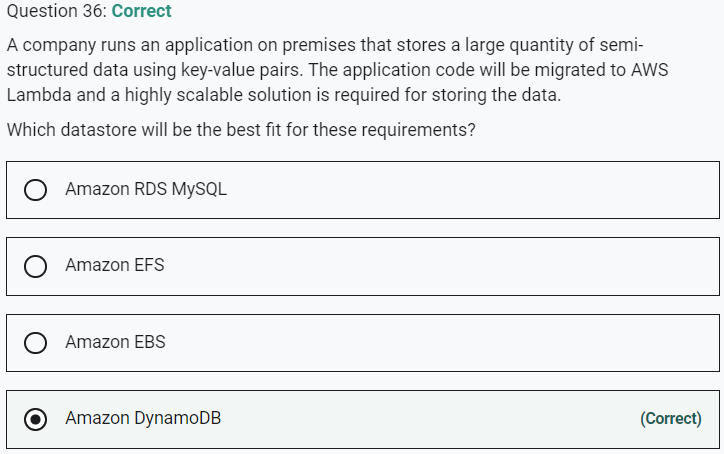




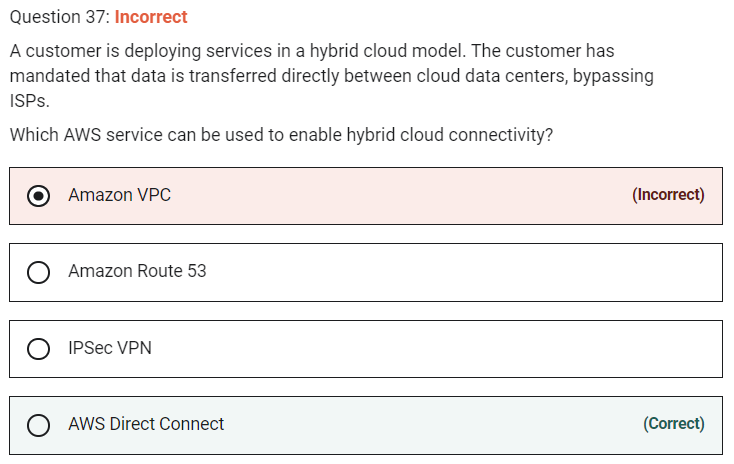
Marked



In this scenario for a stable process that will run constantly on an ongoing basis RIs will be the most affordable solution.

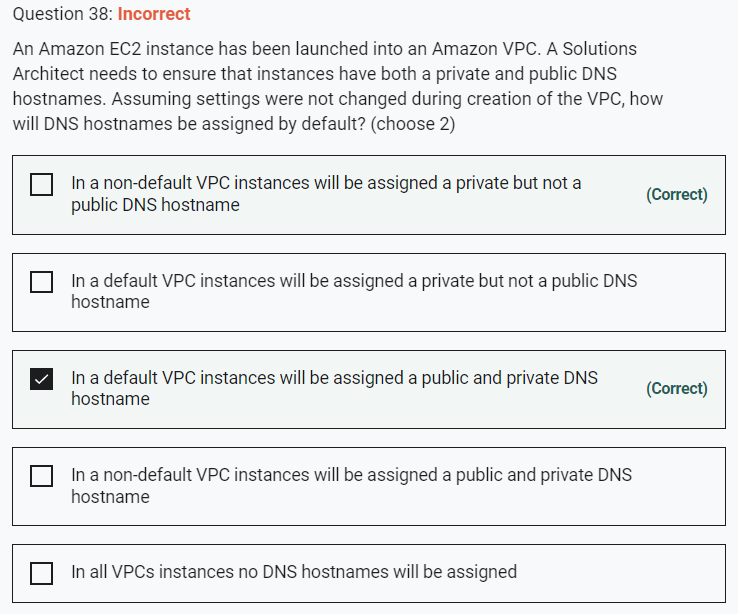


Marked



Bypass Internet – Direct Connect

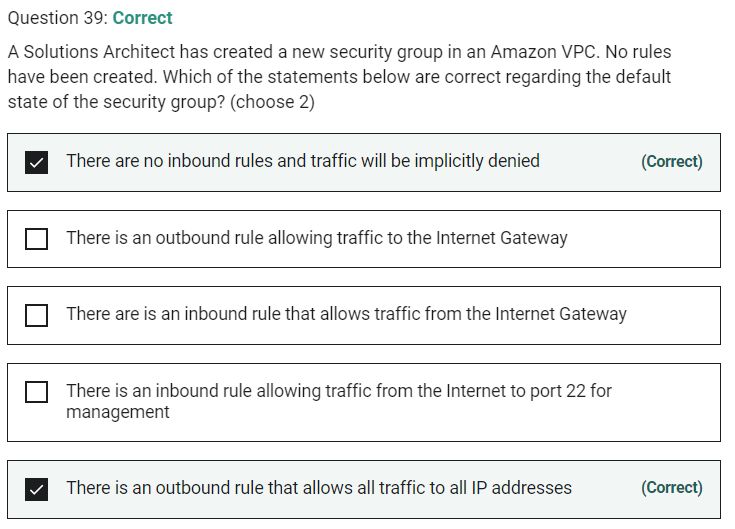
Marked

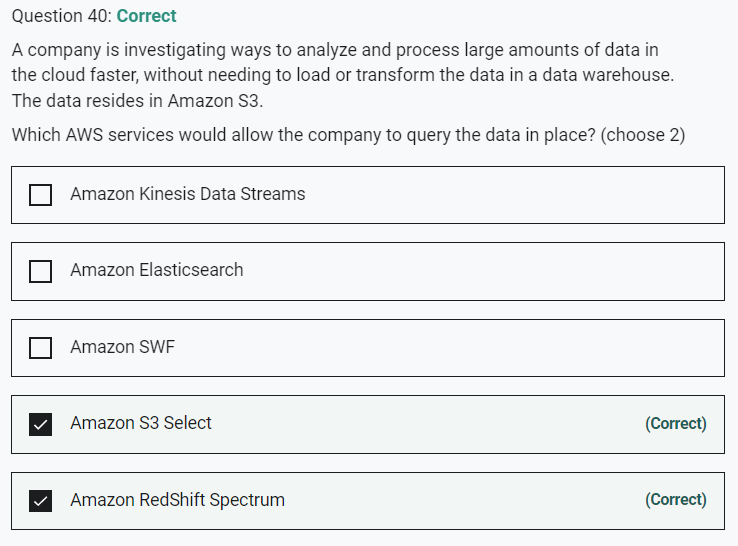


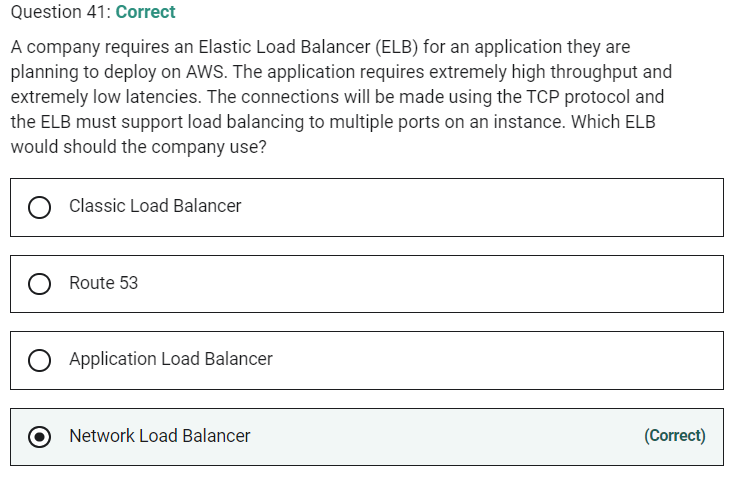
When you launch an instance into a default VPC, we provide the instance with public and private DNS hostnames that correspond to the public IPv4 and private IPv4 addresses for the instance.

When you launch an instance into a nondefault VPC, we provide the instance with a private DNS hostname and we might provide a public DNS hostname, depending on the DNS attributes you specify for the VPC and if your instance has a public IPv4 address.

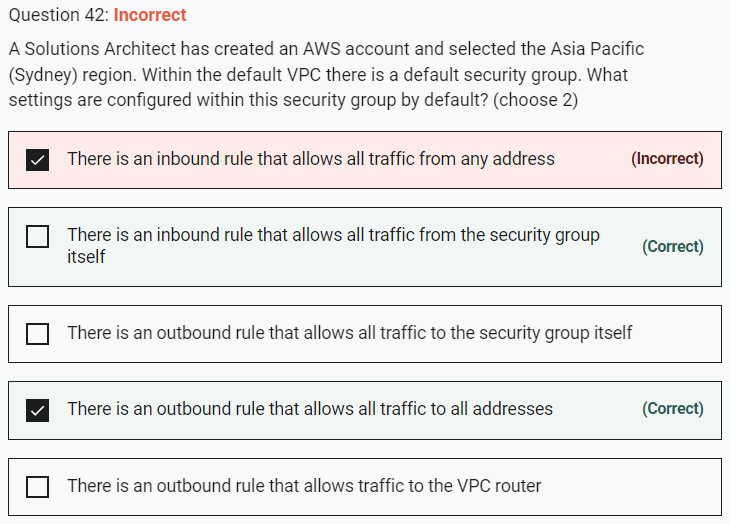
All other statements are incorrect with default settings.





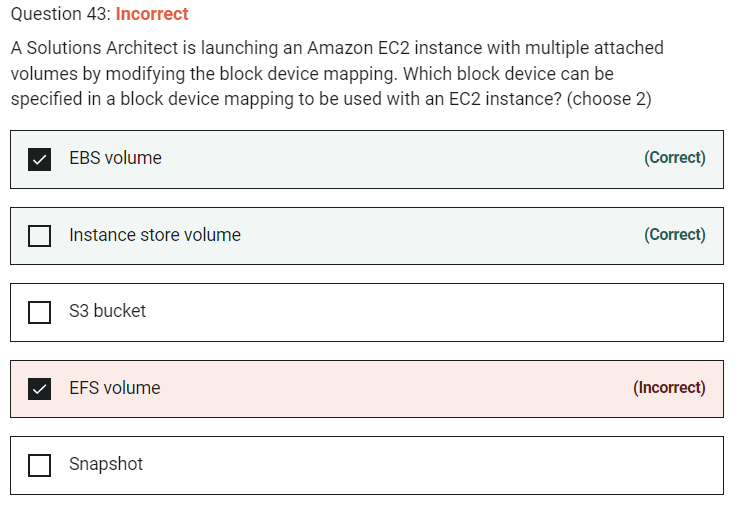


Marked

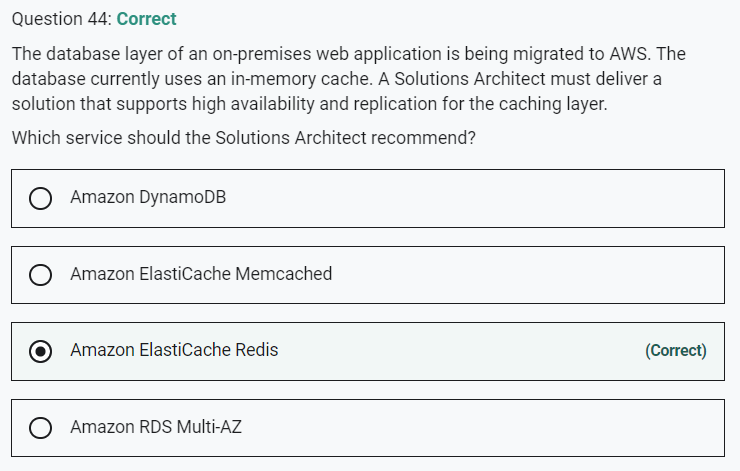


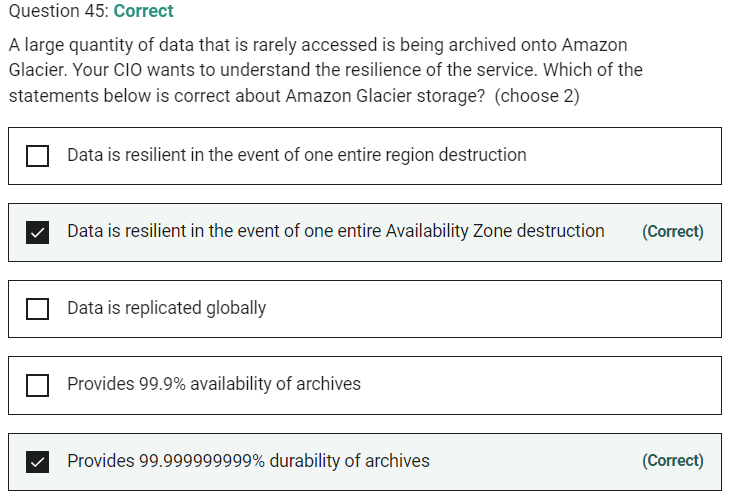
Default security groups have inbound allow rules (allowing traffic from within the group) whereas custom security groups do not have inbound allow rules (all inbound traffic is denied by default). All outbound traffic is allowed by default in custom and default security groups.

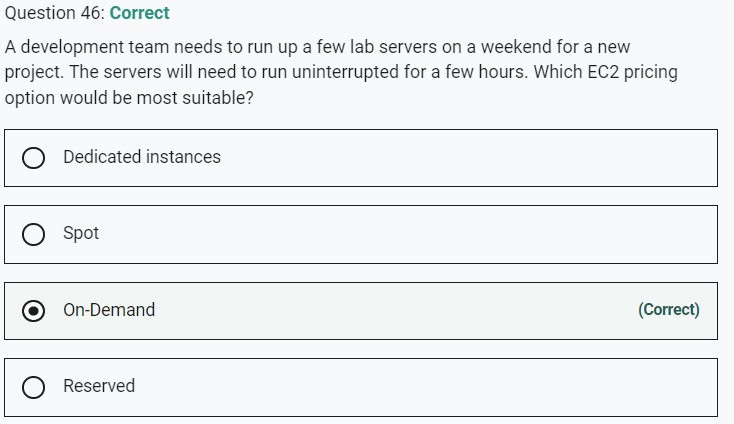
Marked

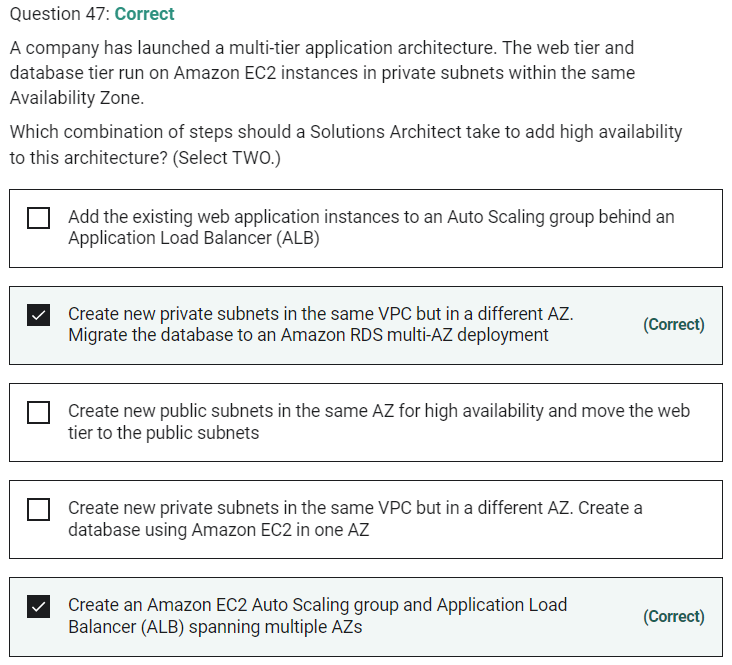


Marked

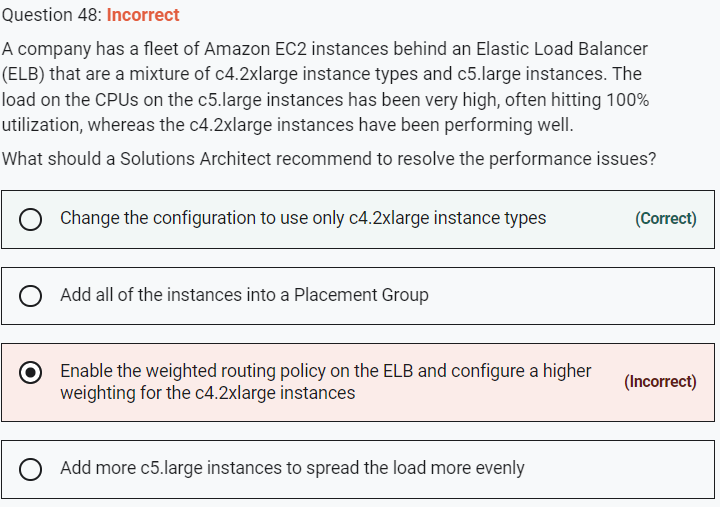








Marked



The 2xlarge instance type provides more CPUs. The best answer is to use this instance type for all instances as the CPU utilization has been lower.

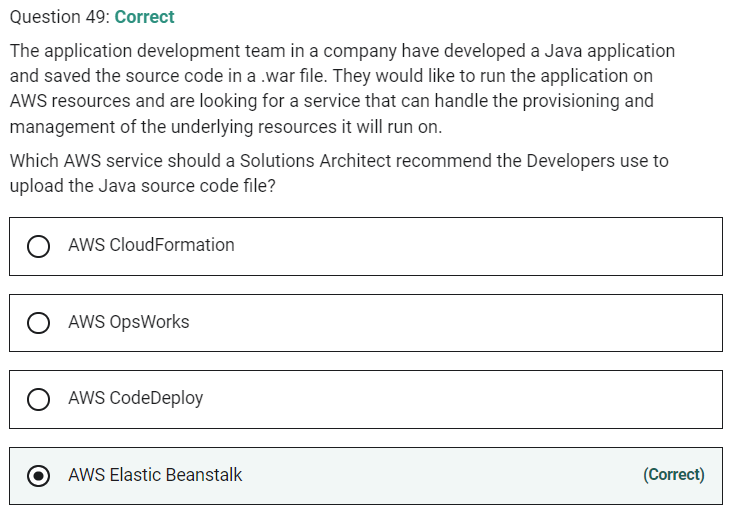
**CORRECT:**"Change the configuration to use only c4.2xlarge instance types" is the correct answer.

**INCORRECT:** "Enable the weighted routing policy on the ELB and configure a higher weighting for the c4.2xlarge instances" is incorrect. The weighted routing policy is a Route 53 feature that would not assist in this situation.

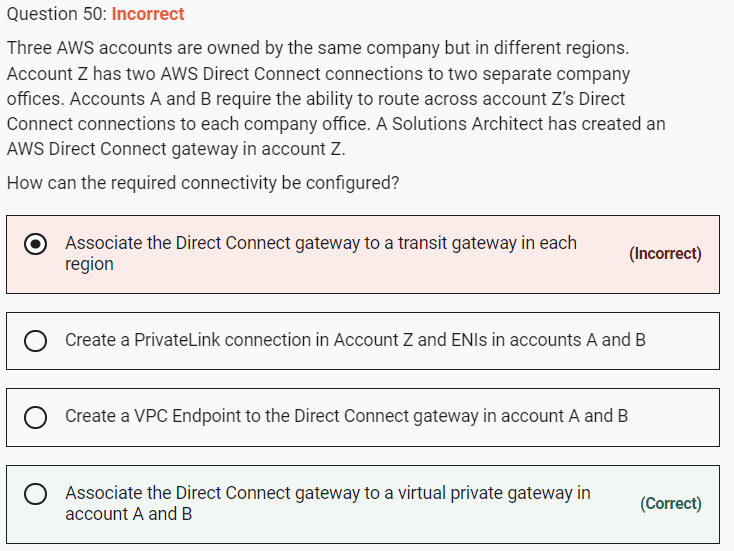
**INCORRECT:** "Add all of the instances into a Placement Group" is incorrect. A placement group helps provide low-latency connectivity between instances and would not help here.

**INCORRECT:** "Add more c5.large instances to spread the load more evenly" is incorrect. This would not help as this instance type is underperforming with high CPU utilization rates.

Marked



Marked

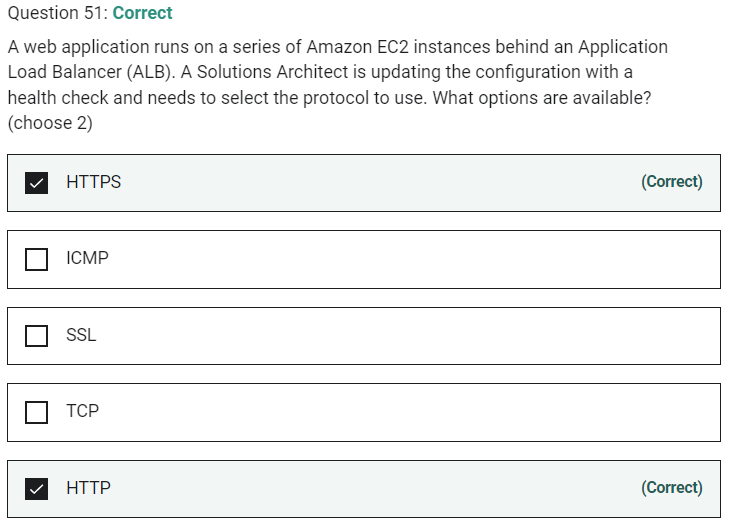


You can associate an AWS Direct Connect gateway with either of the following gateways:

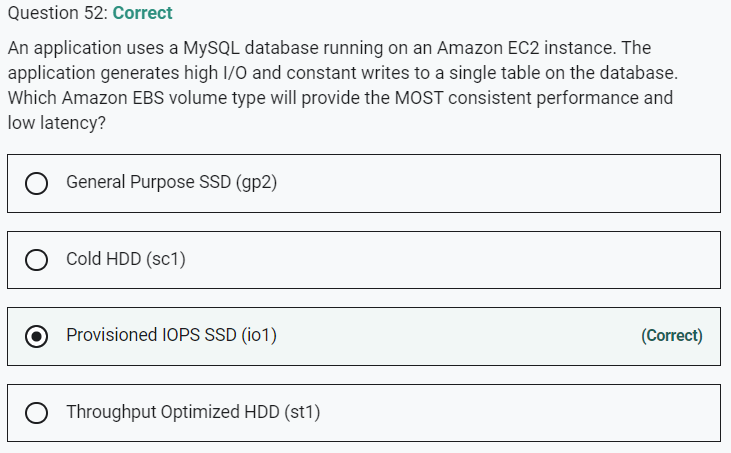
- A transit gateway when you have multiple VPCs in the same Region.

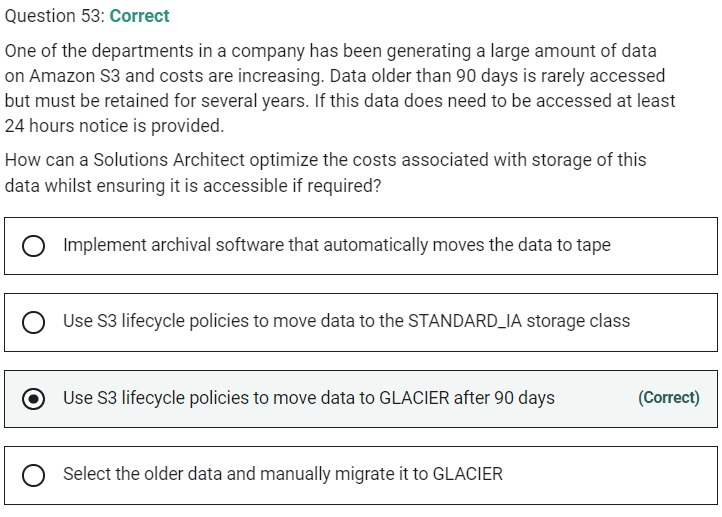
- A virtual private gateway.

In this case account Z owns the Direct Connect gateway so a VPG in accounts A and B must be associated with it to enable this configuration to work. After Account Z accepts the proposals, Account A and Account B can route traffic from their virtual private gateway to the Direct Connect gateway.

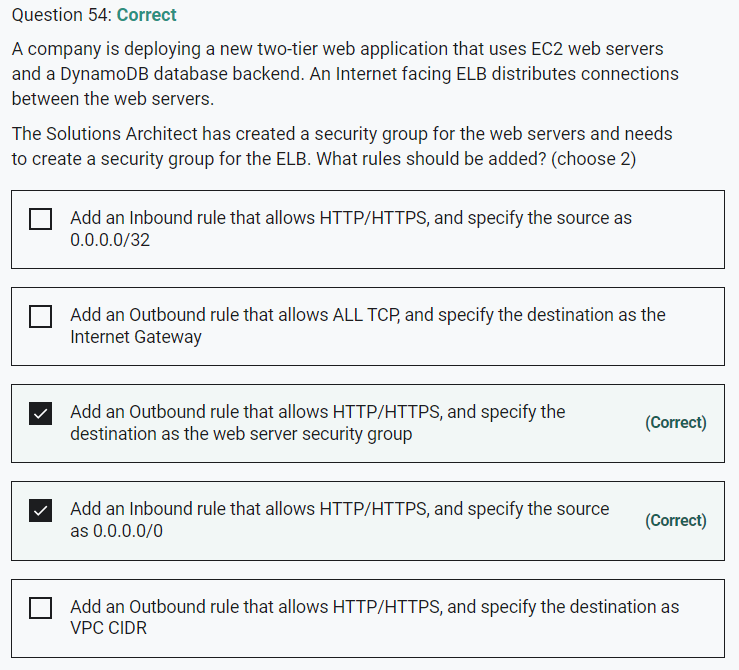


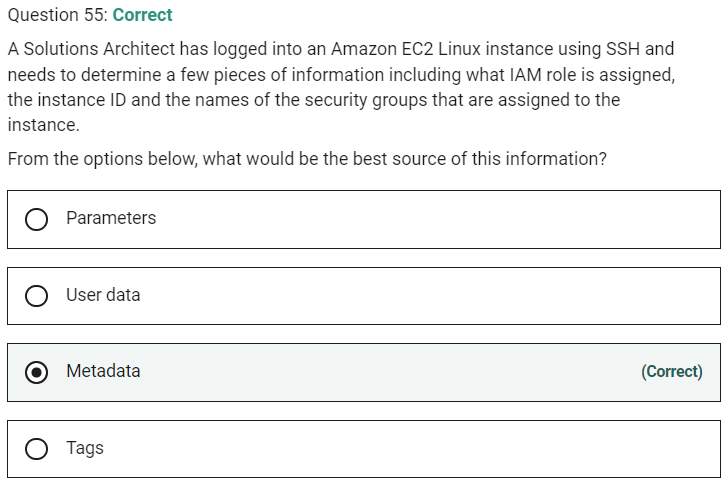
Marked



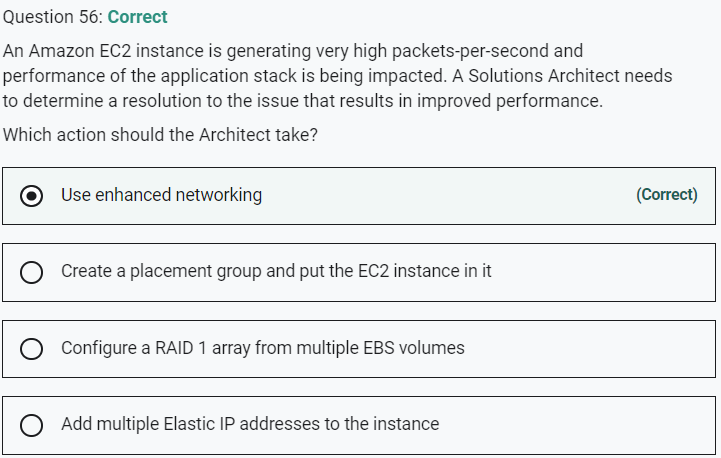


Marked

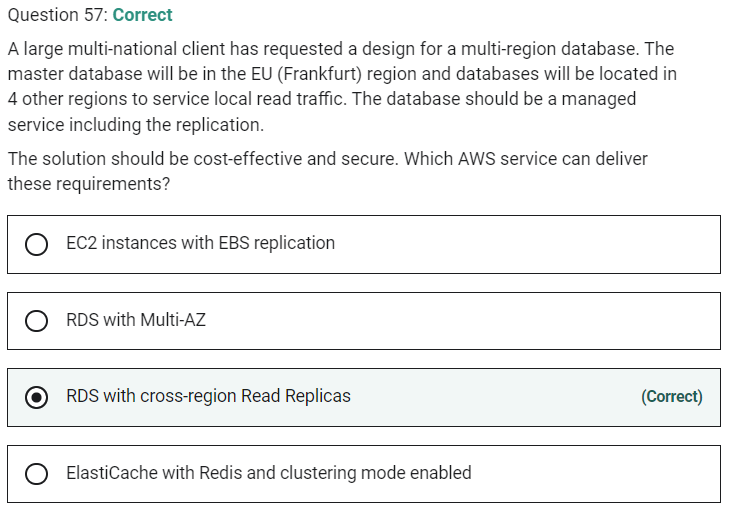




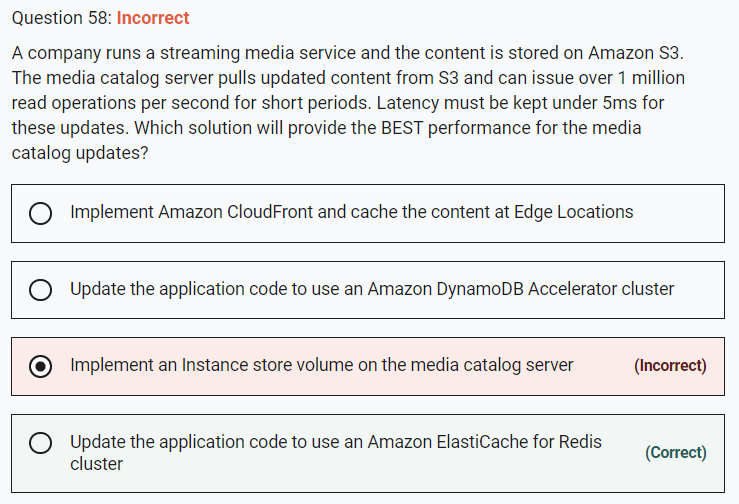
Marked



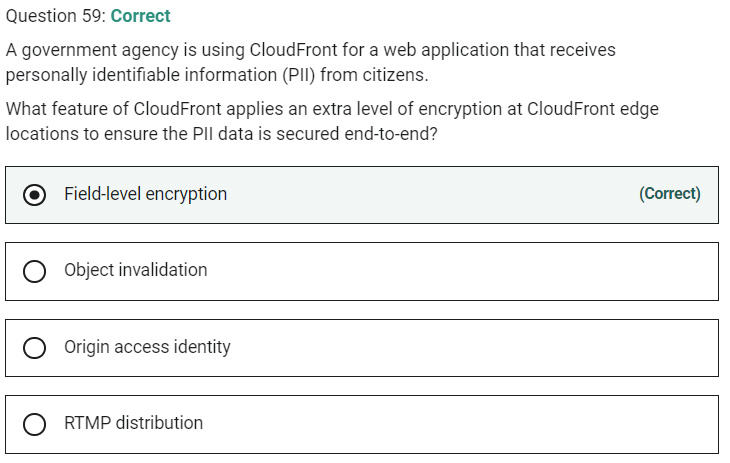
Marked

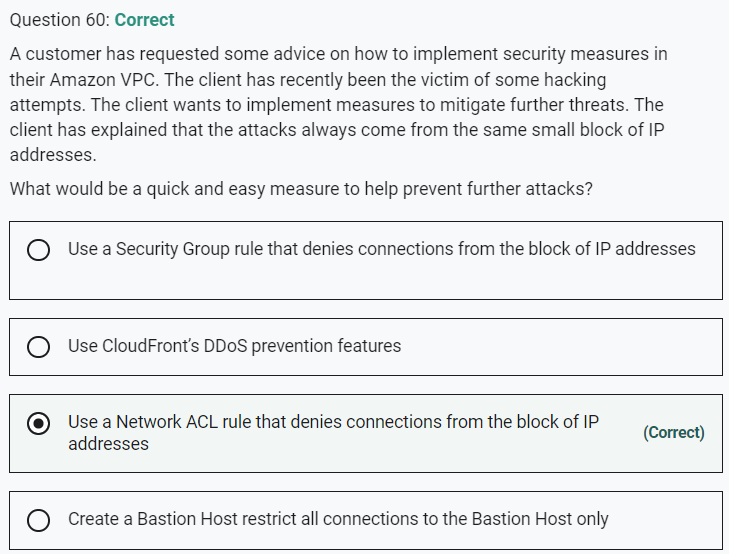


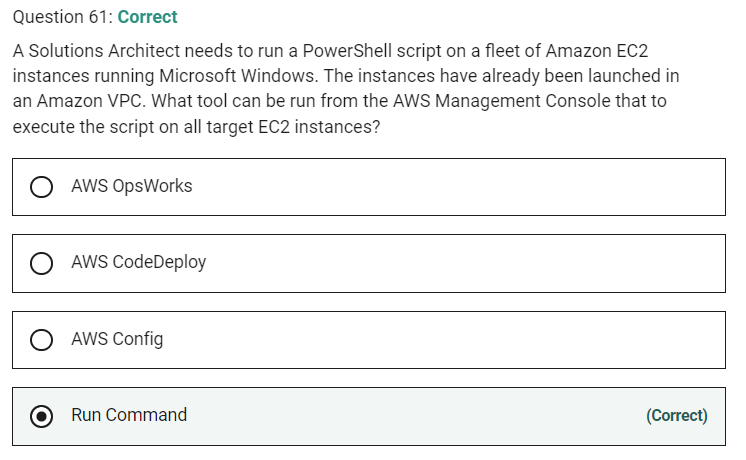
Marked



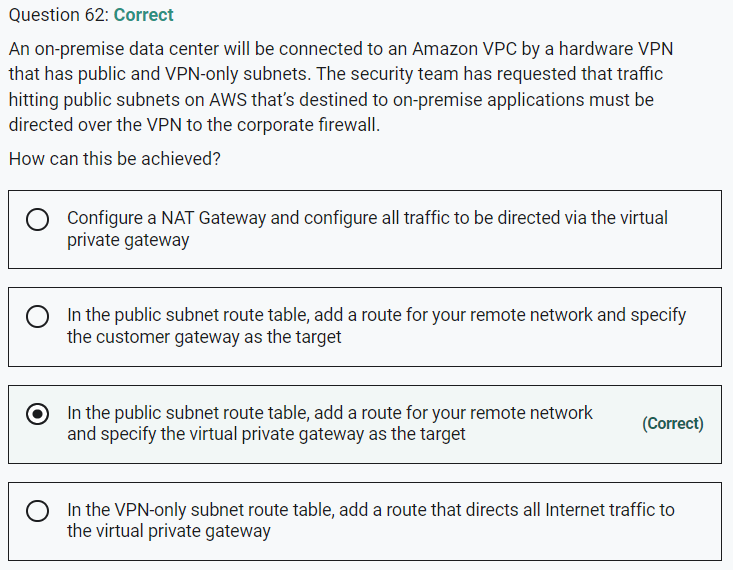
**INCORRECT:** "Implement Amazon CloudFront and cache the content at Edge Locations" is incorrect. CloudFront is good for getting media closer to users but in this case we’re trying to improve performance within the data center moving data from S3 to the media catalog server.



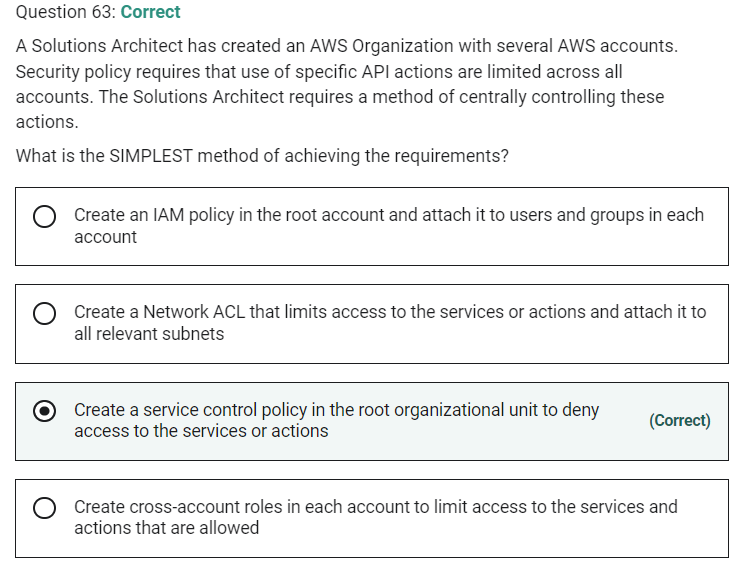




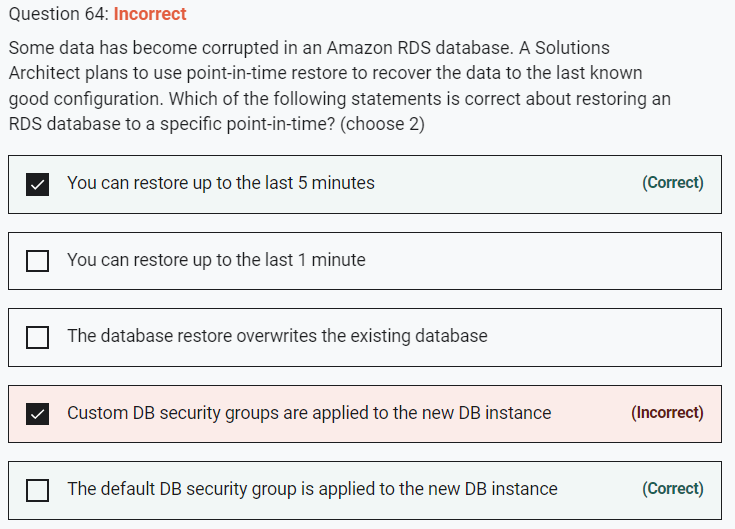
Marked



Route tables determine where network traffic is directed. In your route table, you must add a route for your remote network and specify the virtual private gateway as the target. This enables traffic from your VPC that’s destined for your remote network to route via the virtual private gateway and over one of the VPN tunnels. You can enable route propagation for your route table to automatically propagate your network routes to the table for you.



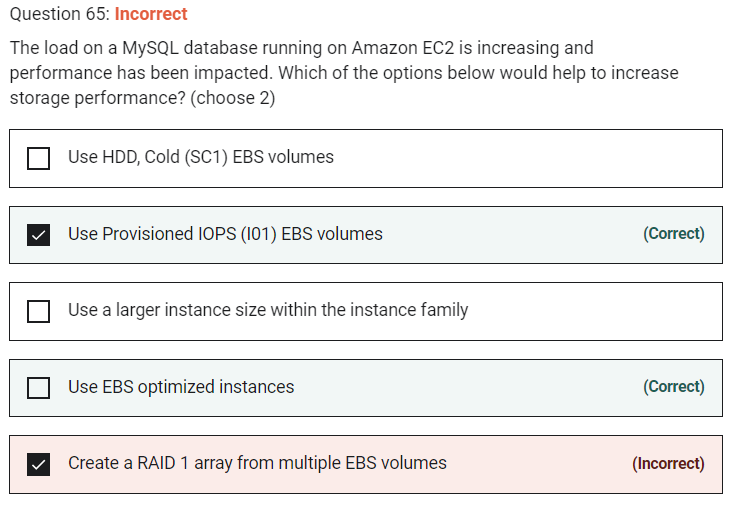
Marked



You can restore a DB instance to a specific point in time, creating a new DB instance. When you restore a DB instance to a point in time, the default DB security group is applied to the new DB instance. If you need custom DB security groups applied to your DB instance, you must apply them explicitly using the AWS Management Console, the AWS CLI modify-db-instance command, or the Amazon RDS API ModifyDBInstance operation after the DB instance is available.

Restored DBs will always be a new RDS instance with a new DNS endpoint and you can restore up to the last 5 minutes.

Marked



EBS optimized instances provide dedicated capacity for Amazon EBS I/O. EBS optimized instances are designed for use with all EBS volume types.

Provisioned IOPS EBS volumes allow you to specify the amount of IOPS you require up to 50 IOPS per GB. Within this limitation you can therefore choose to select the IOPS required to improve the performance of your volume.

RAID can be used to increase IOPS, however RAID 1 does not. For example:

– RAID 0 = 0 striping – data is written across multiple disks and increases performance but no redundancy.

– RAID 1 = 1 mirroring – creates 2 copies of the data but does not increase performance, only redundancy.

HDD, Cold – (SC1) provides the lowest cost storage and low performance