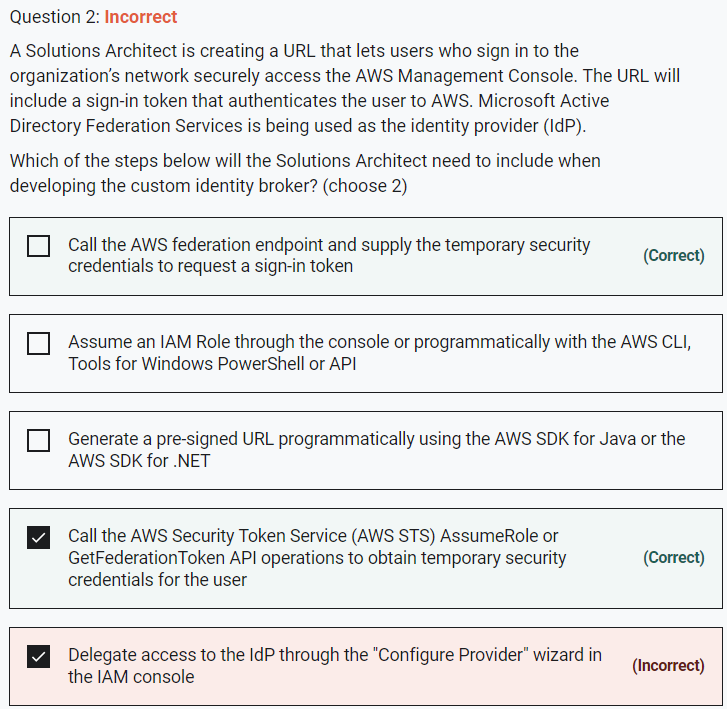
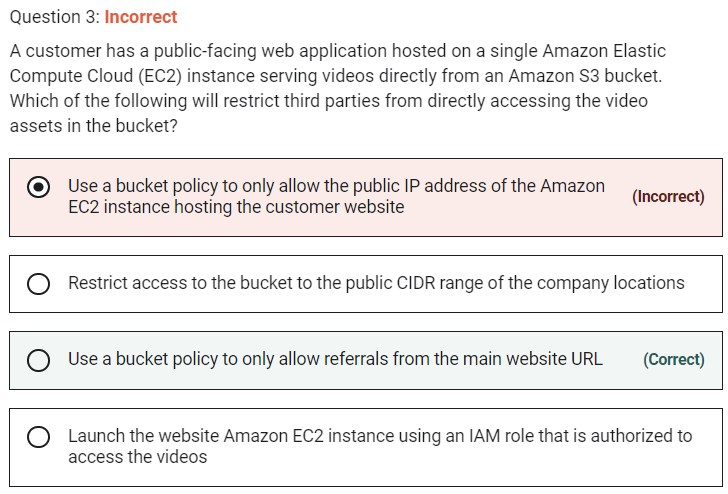
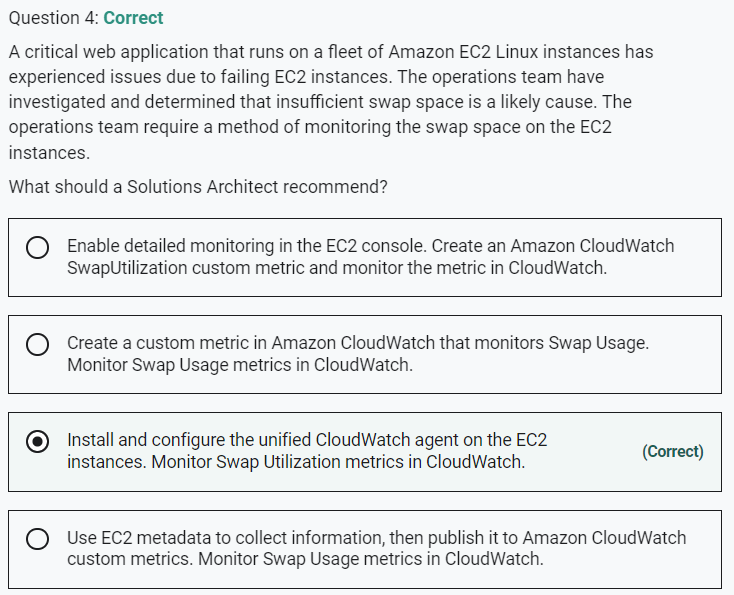


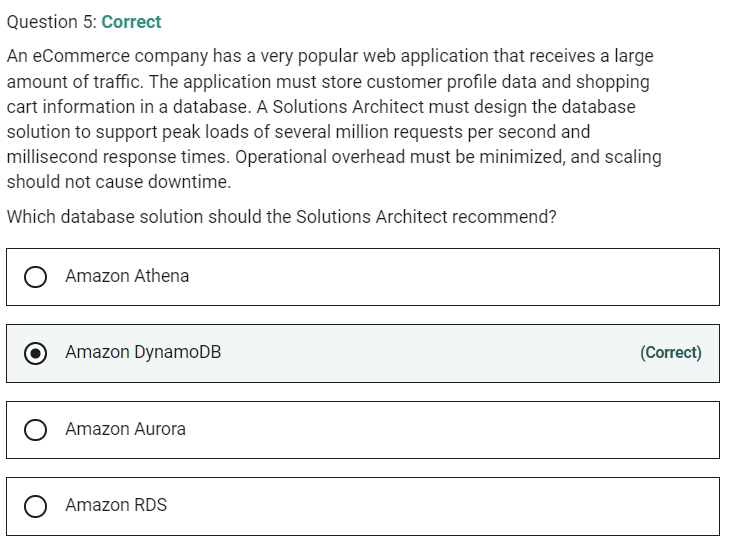
Marked



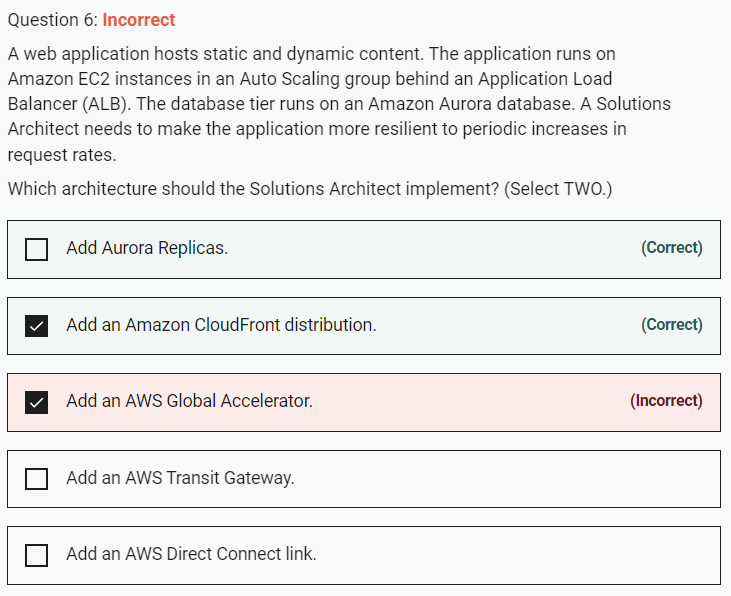
Marked

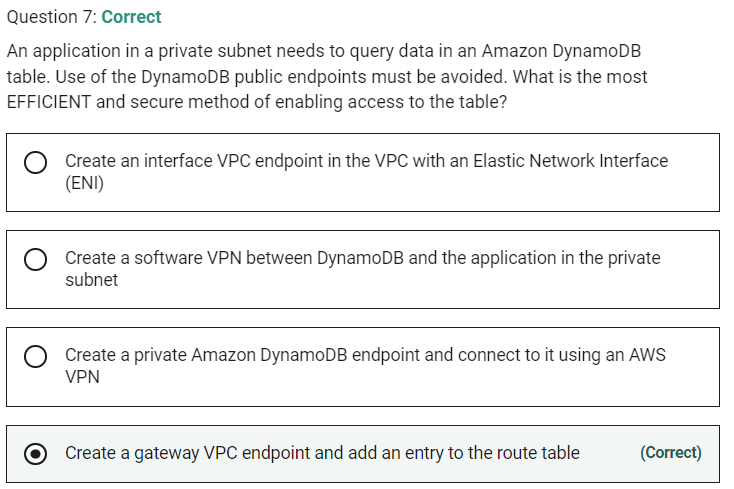


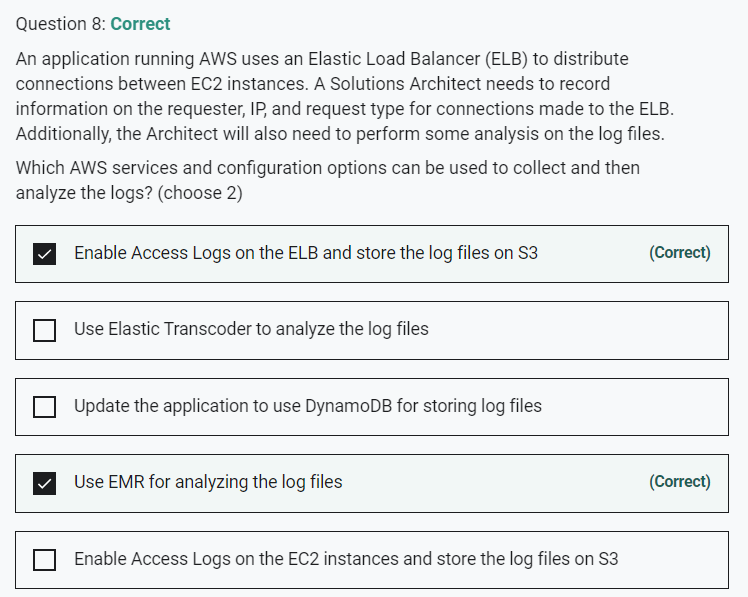


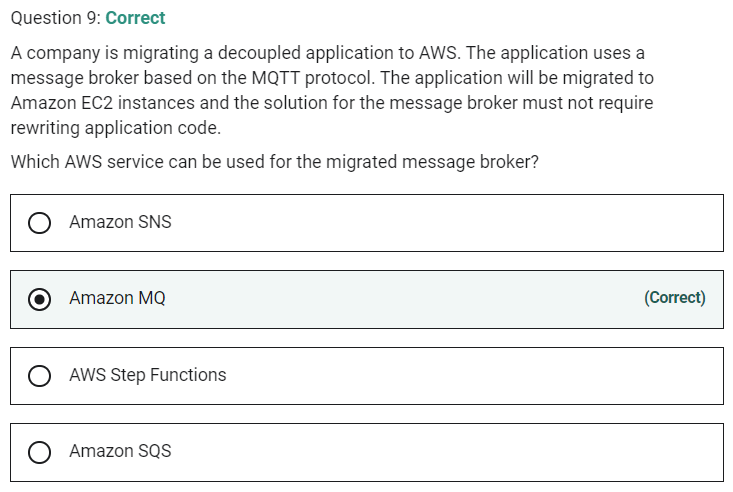


Marked

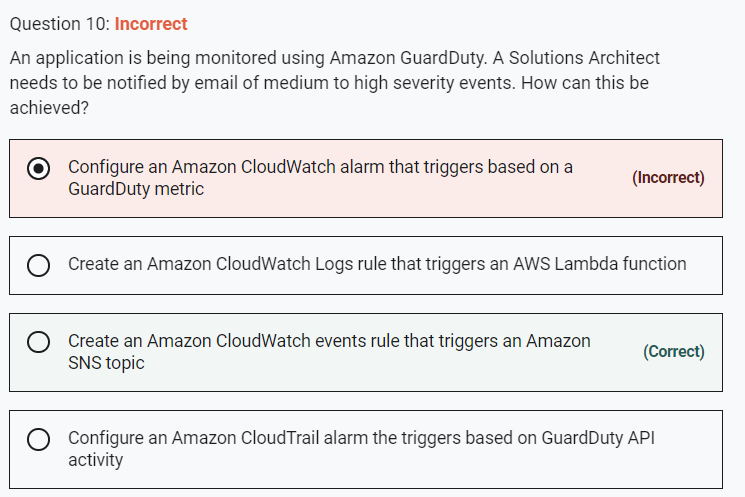




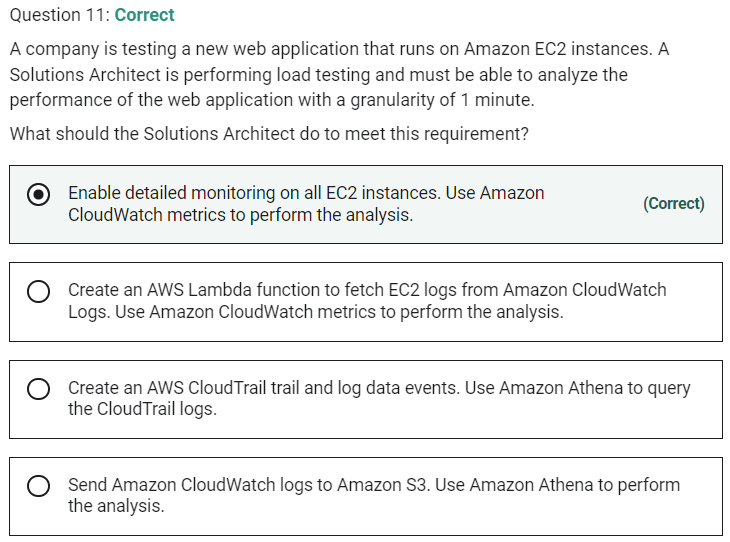




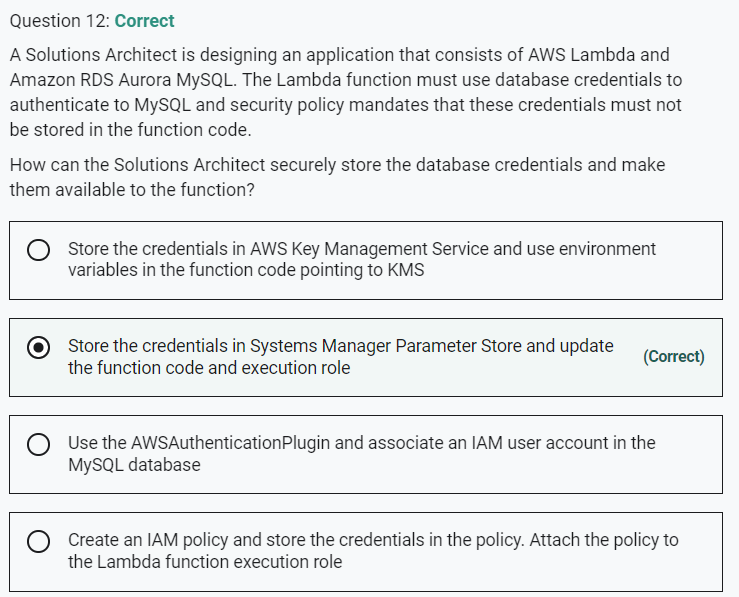
Marked

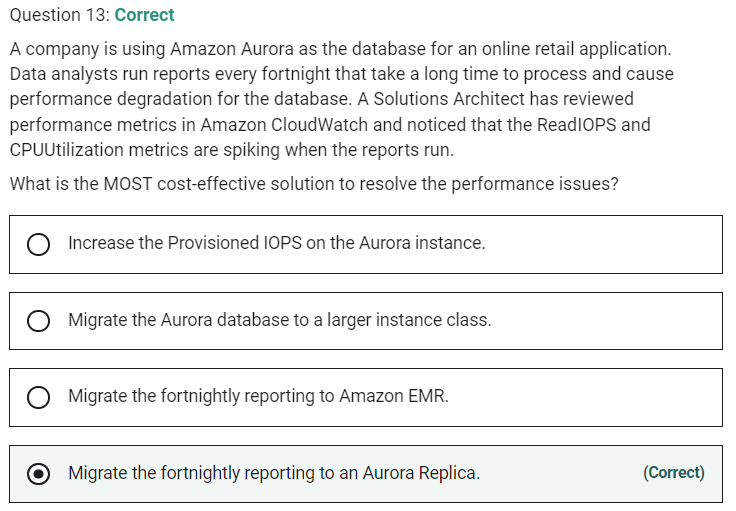


There is nothing like guardduty metric

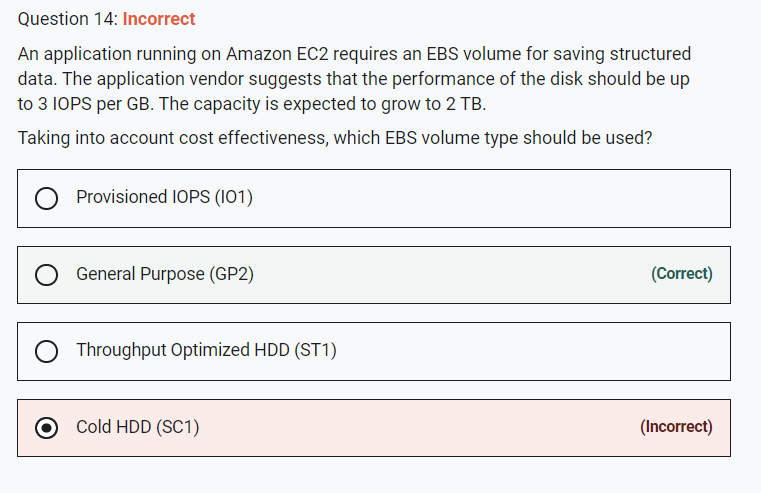


Marked



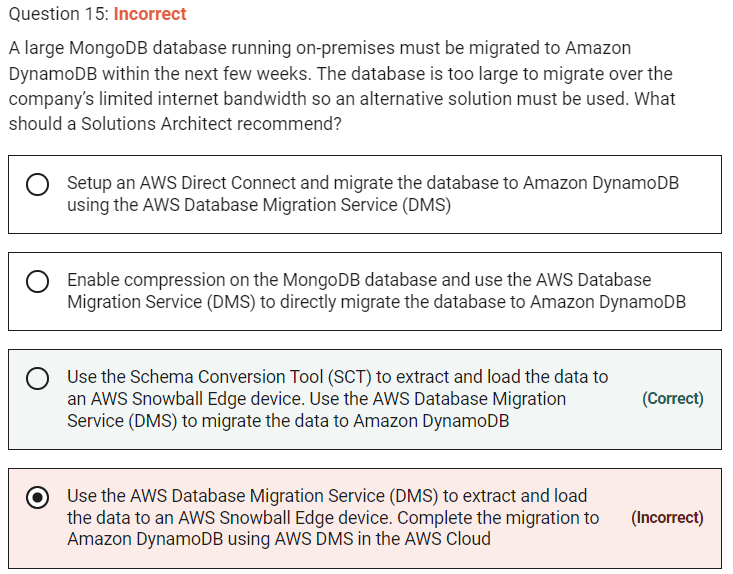


Marked



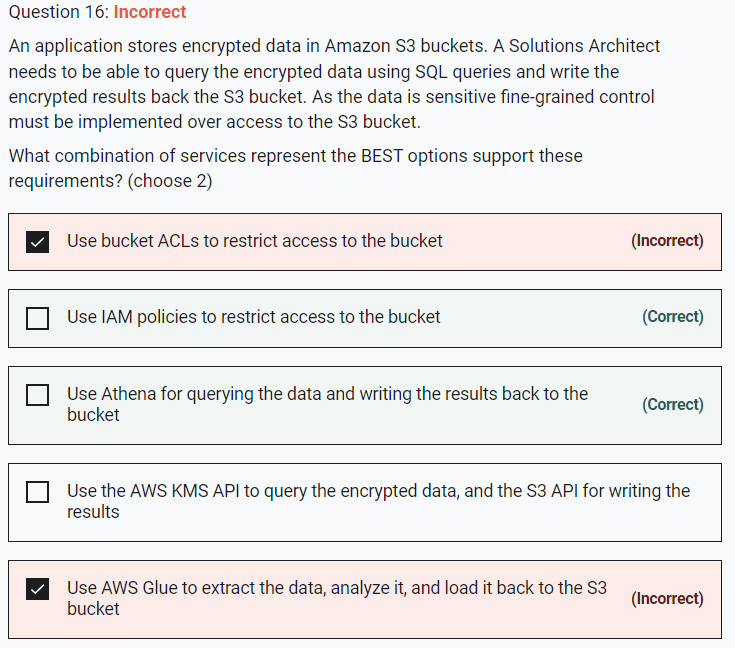
SSD, General Purpose (GP2) provides enough IOPS to support this requirement and is the most economical option that does. Using Provisioned IOPS would be more expensive and the other two options do not provide an SLA for IOPS.

Marked

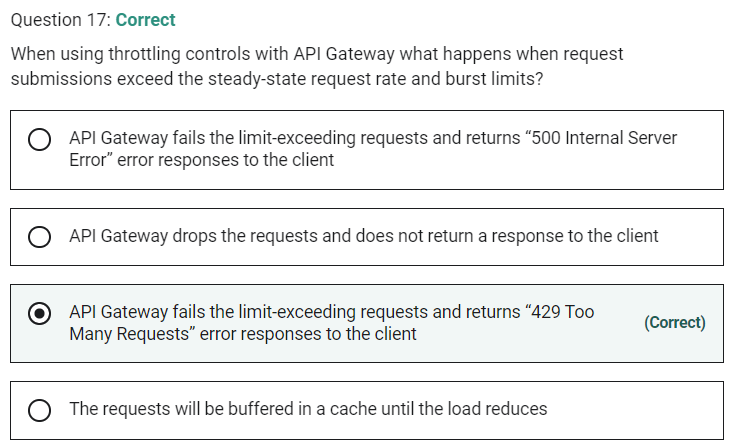


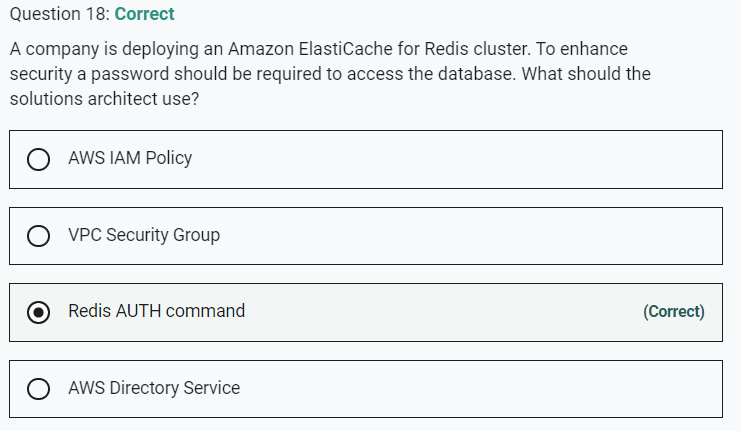
**INCORRECT:** "Use the AWS Database Migration Service (DMS) to extract and load the data to an AWS Snowball Edge device. Complete the migration to Amazon DynamoDB using AWS DMS in the AWS Cloud" is incorrect. This is the wrong method, the Solutions Architect should use the SCT to extract and load to Snowball Edge and then AWS DMS in the AWS Cloud.

Marked

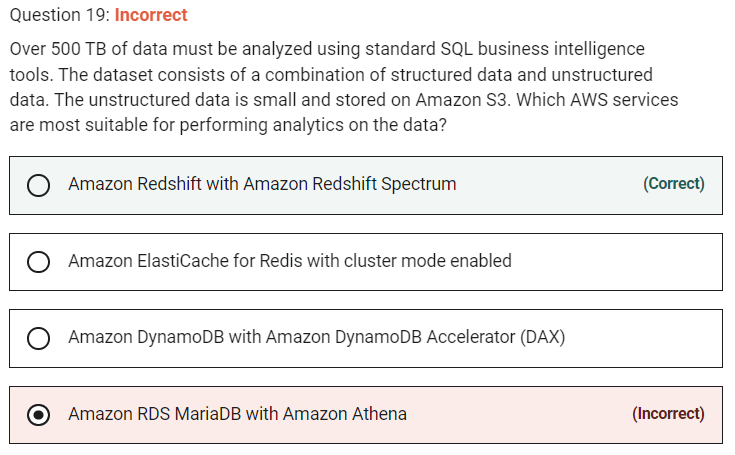


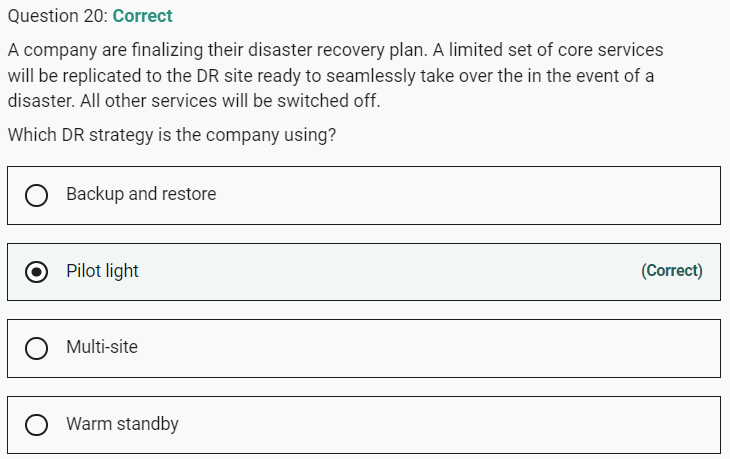
Athena allows you to easily query encrypted data stored in Amazon S3 and write encrypted results back to your S3 bucket. Both, server-side encryption and client-side encryption are supported.



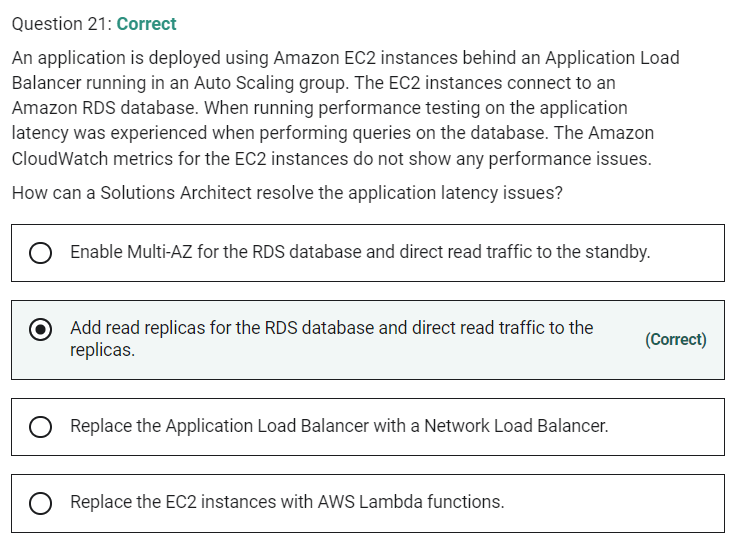


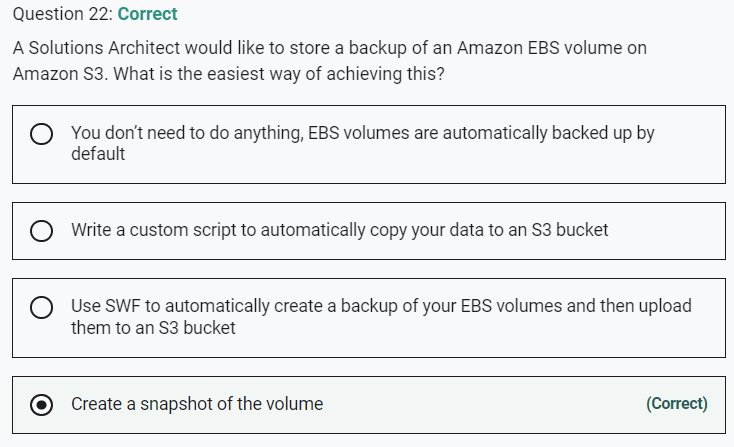
Marked



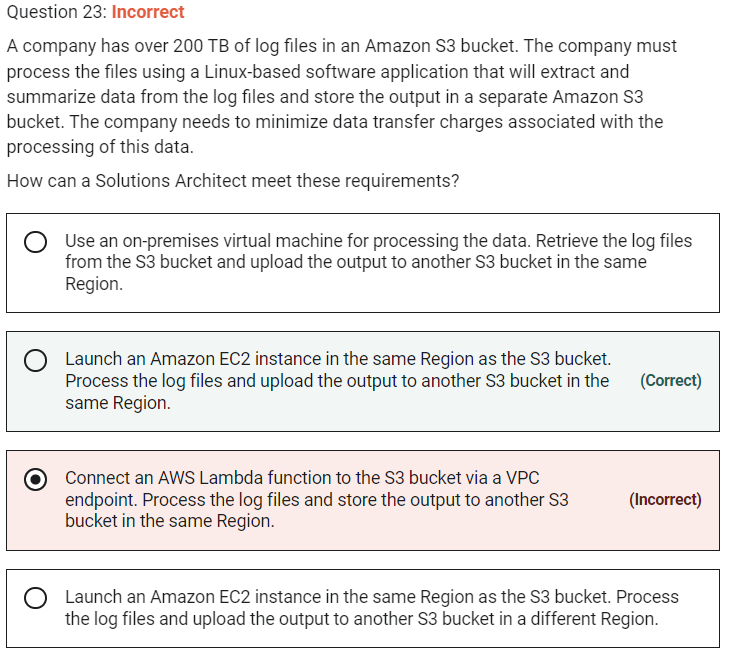


Marked





Marked



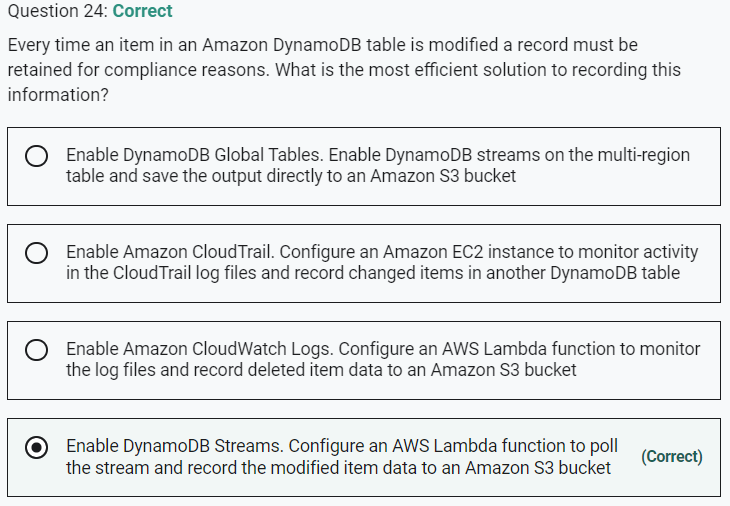
The software application must be installed on a Linux operating system so we must use Amazon EC2 or an on-premises VM. To avoid data charges however, we must ensure that the data does not egress the AWS Region. The best solution to avoid the egress data charges is to use an Amazon EC2 instance in the same Region as the S3 bucket that contains the log files. The processed output files must also be stored in a bucket in the same Region to avoid any data going out from EC2 to another Region.

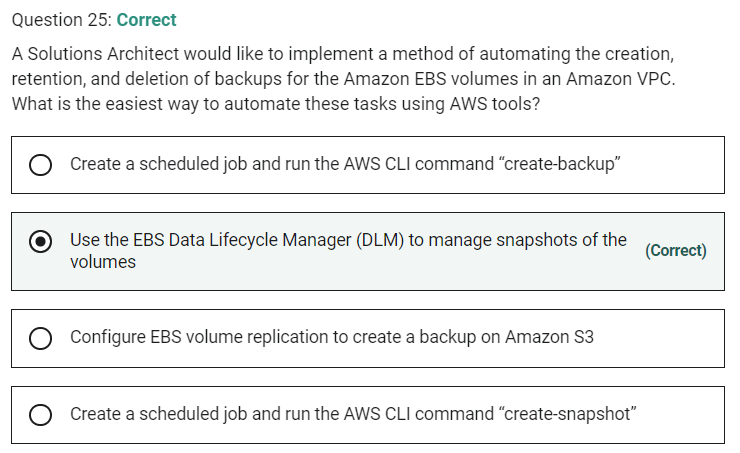
**CORRECT:**"Launch an Amazon EC2 instance in the same Region as the S3 bucket. Process the log files and upload the output to another S3 bucket in the same Region" is the correct answer.

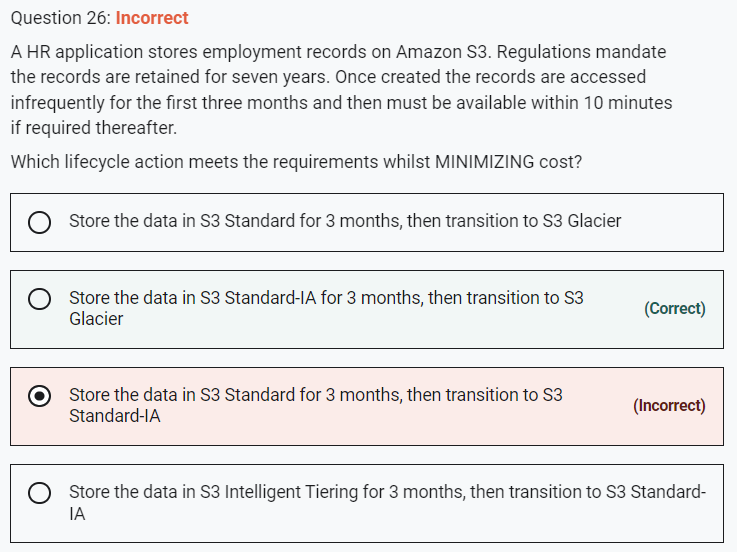
**INCORRECT:** "Use an on-premises virtual machine for processing the data. Retrieve the log files from the S3 bucket and upload the output to another S3 bucket in the same Region" is incorrect. The data would need to egress the AWS Region incurring data transfer charges in this configuration.

**INCORRECT:** "Launch an Amazon EC2 instance in the same Region as the S3 bucket. Process the log files and upload the output to another S3 bucket in a different Region" is incorrect. The processed data would be going from the EC2 instance to a bucket in a different Region which would incur data transfer charges.

**INCORRECT:** "Connect an AWS Lambda function to the S3 bucket via a VPC endpoint. Process the log files and store the output to another S3 bucket in the same Region" is incorrect. You cannot install a Linux-based software application on AWS Lambda.

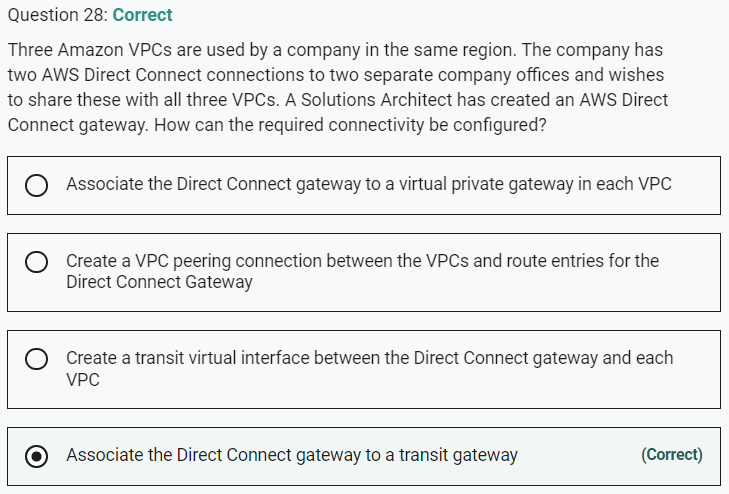


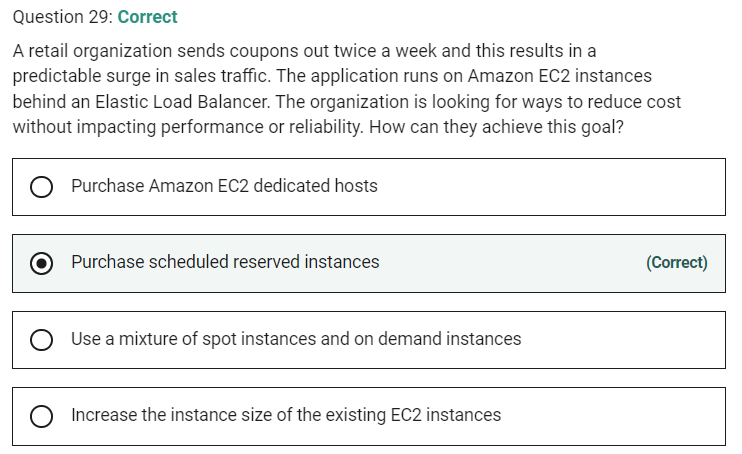




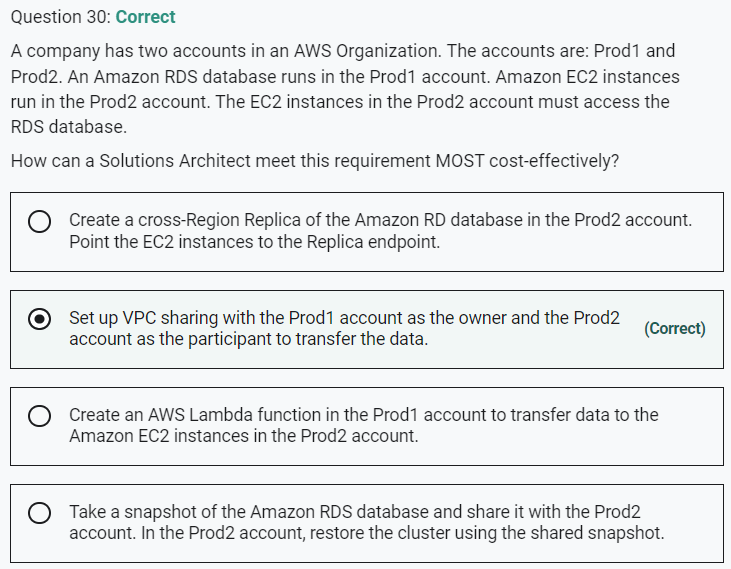


Marked

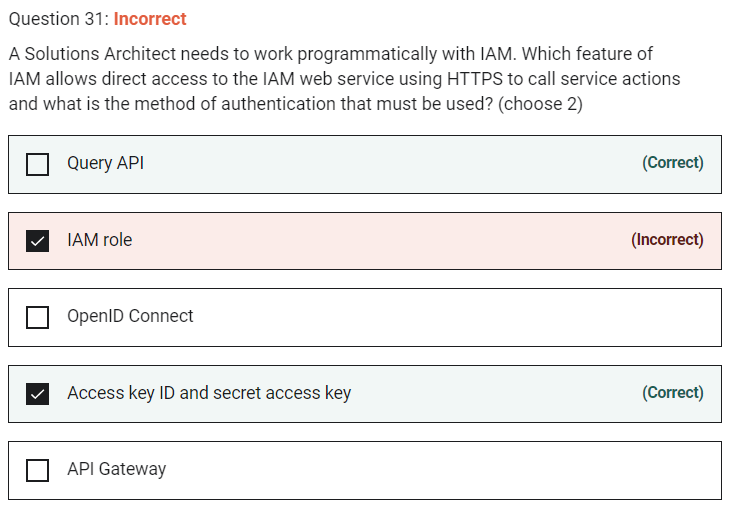




Marked

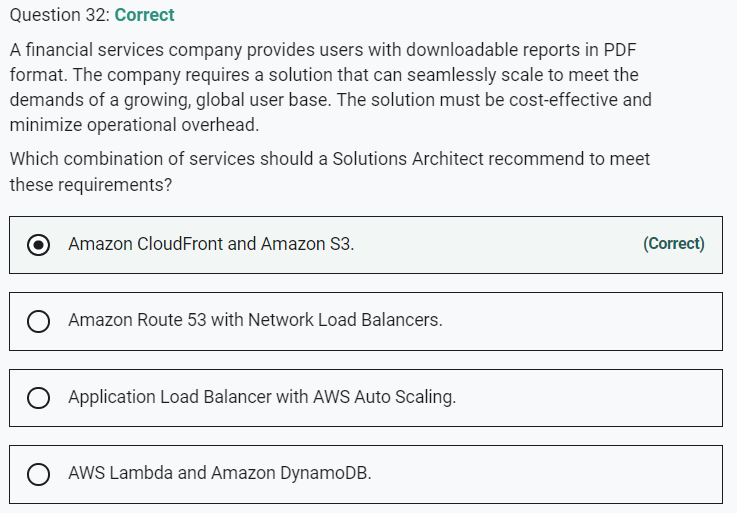


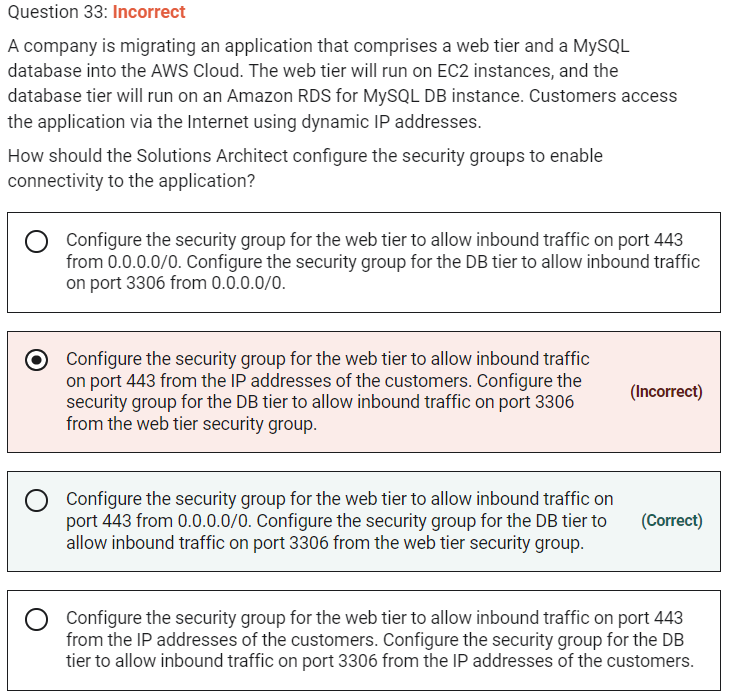
Marked

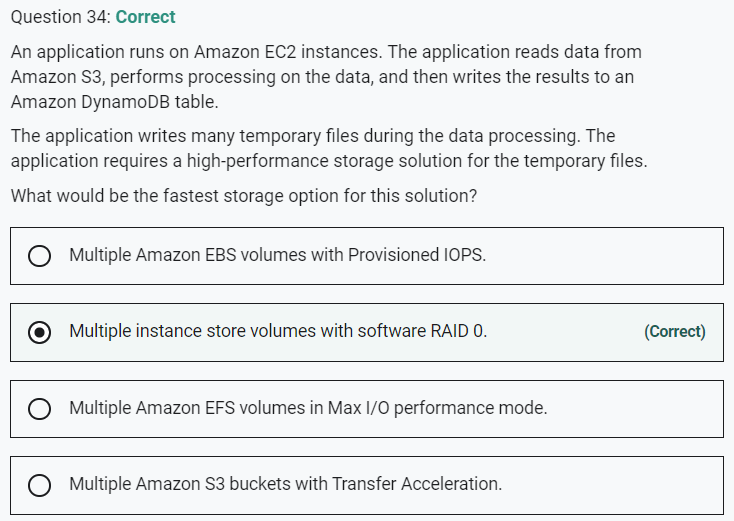


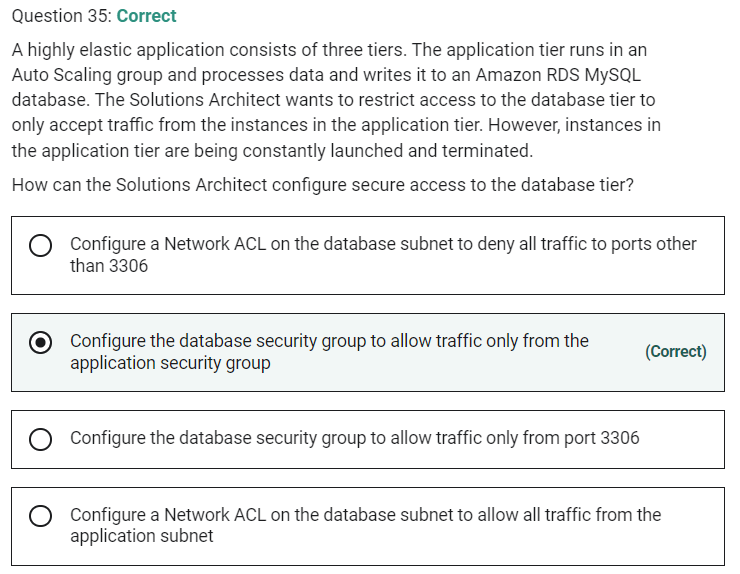
AWS recommend that you use the AWS SDKs to make programmatic API calls to IAM. However, you can also use the IAM Query API to make direct calls to the IAM web service. An access key ID and secret access key must be used for authentication when using the Query API.

Marked









Marked



Policies are documents that define permissions and can be applied to users, groups and roles. Policy documents are written in JSON (key value pair that consists of an attribute and a value).

Within an IAM policy you can grant either programmatic access or AWS Management Console access to Amazon S3 resources.

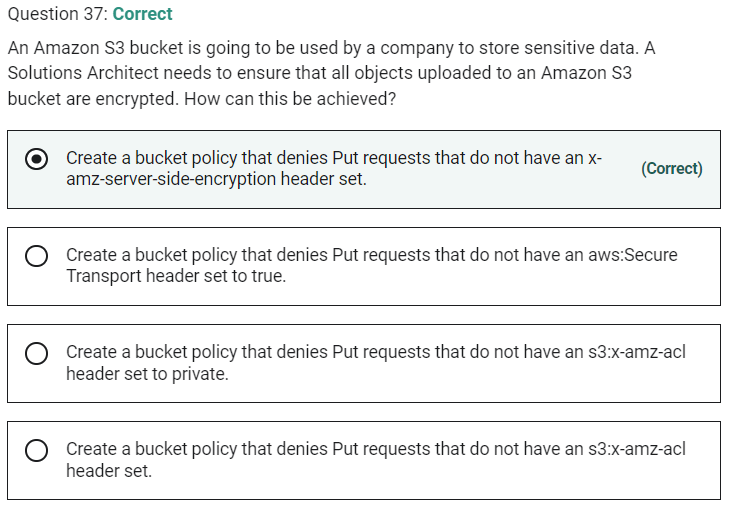
**CORRECT:**"Grant programmatic access" is a correct answer.

**CORRECT:**"Create an IAM policy" is also a correct answer.

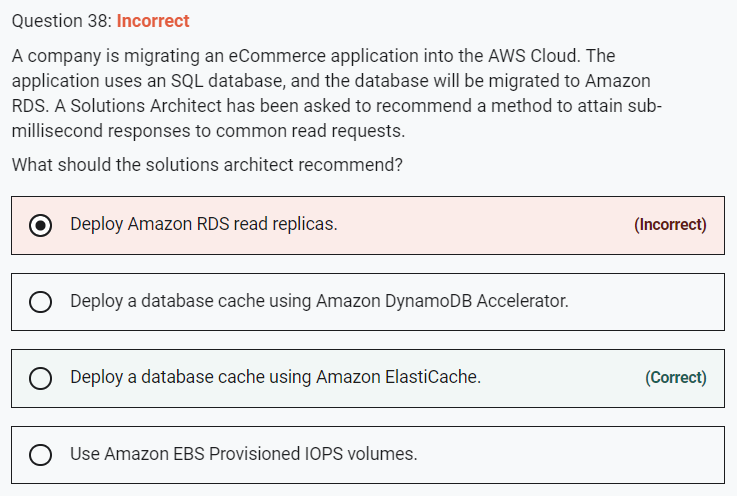
**INCORRECT:** "Create a bucket policy" is incorrect as it is more efficient to use an IAM policy.

**INCORRECT:** "Use key pairs" is incorrect. Key pairs are used for access to EC2 instances; a bucket policy would not assist with access control with EC2 and granting management console access will not assist the application which is making API calls to the services.

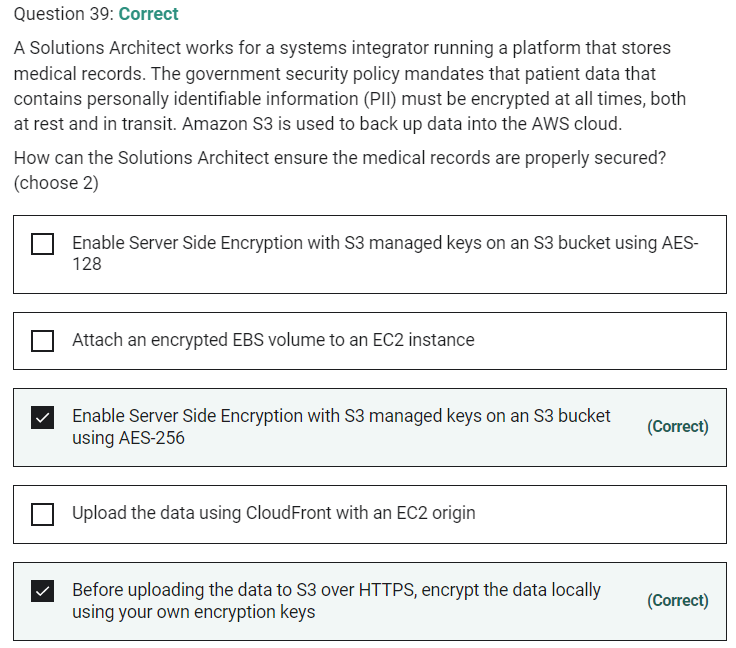
**INCORRECT:** "Grant AWS Management Console access" is incorrect as programmatic access is required.



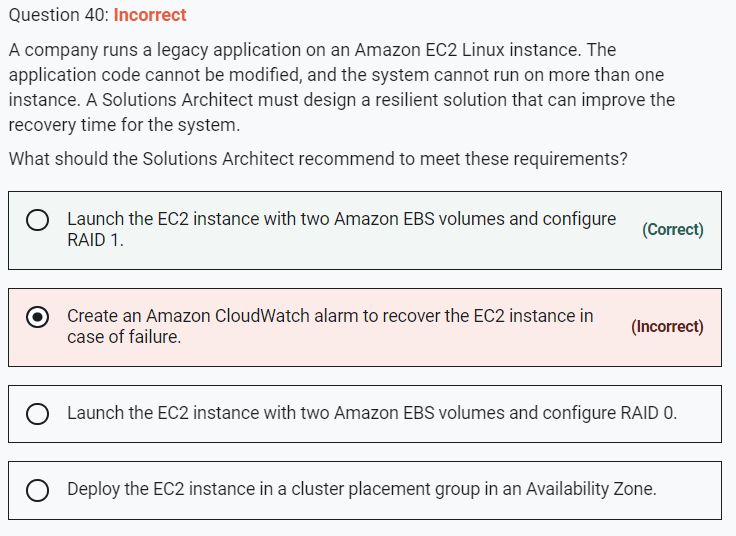
Marked



Read replicas will not provide sub-millisecond response times to queries.

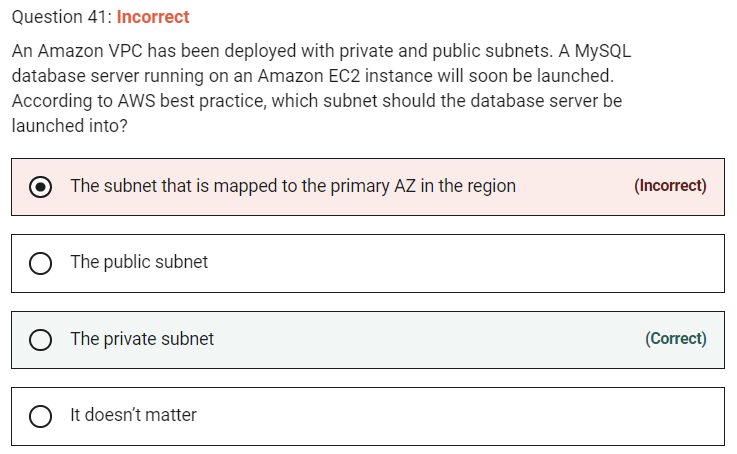


Marked



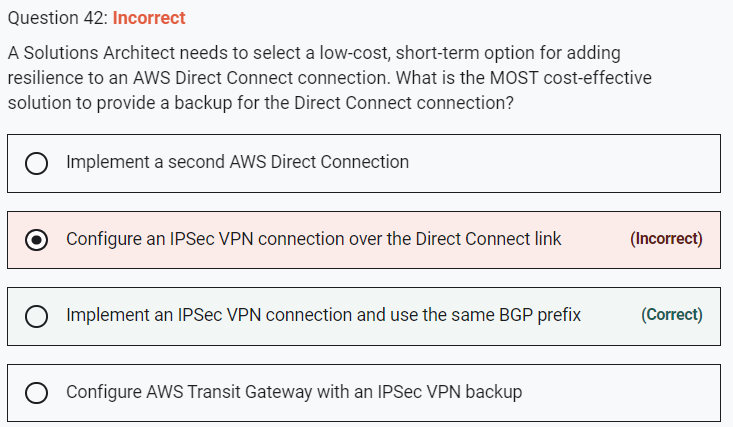
**INCORRECT:** "Create an Amazon CloudWatch alarm to recover the EC2 instance in case of failure" is incorrect. This does not improve recovery time it just attempts to fix issues relating to the underlying hardware.

**INCORRECT:** "Deploy the EC2 instance in a cluster placement group in an Availability Zone" is incorrect. You cannot gain any advantages by deploying a single instance into a cluster placement group.

marked

AWS best practice is to deploy databases into private subnets wherever possible. You can then deploy your web front-ends into public subnets and configure these, or an additional application tier to write data to the database.

Marked



This is the most cost-effective solution. With this option both the Direct Connect connection and IPSec VPN are active and being advertised using the Border Gateway Protocol (BGP). The Direct Connect link will always be preferred unless it is unavailable.

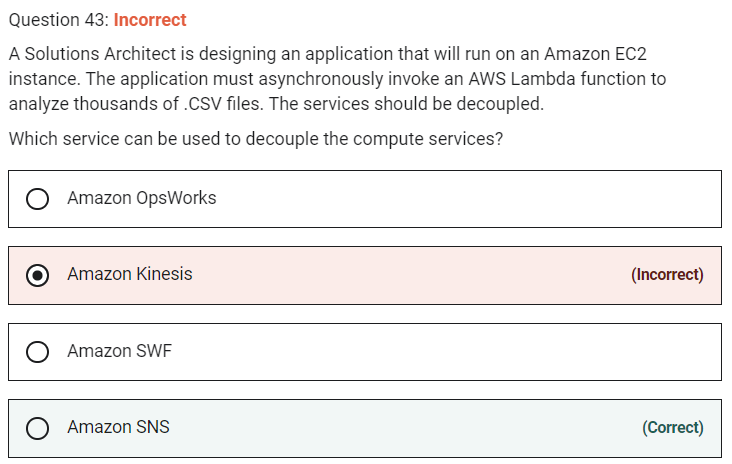
**CORRECT:**"Implement an IPSec VPN connection and use the same BGP prefix" is the correct answer.

**INCORRECT:** "Implement a second AWS Direct Connection" is incorrect. This is not a short-term or low-cost option as it takes time to implement and is costly.

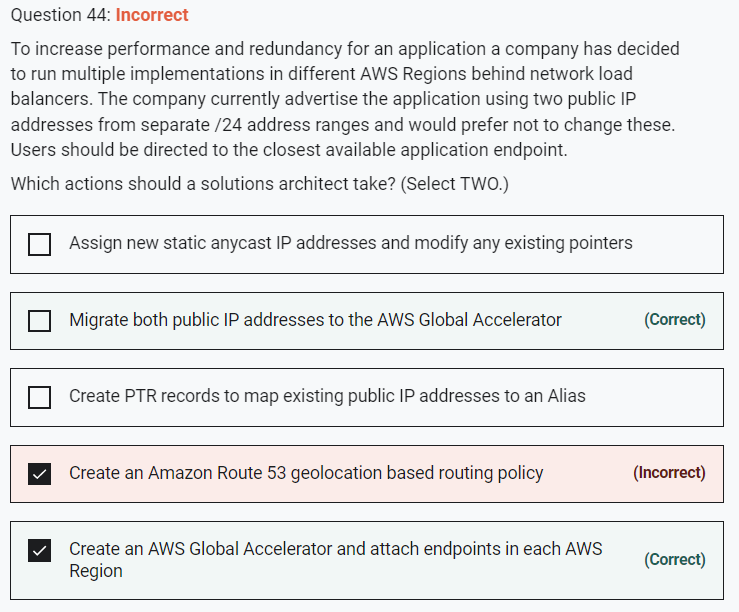
**INCORRECT:** "Configure AWS Transit Gateway with an IPSec VPN backup" is incorrect. This is a workable solution and provides some advantages. However, you do need to pay for the Transit Gateway so it is not the most cost-effective option and probably not suitable for a short-term need.

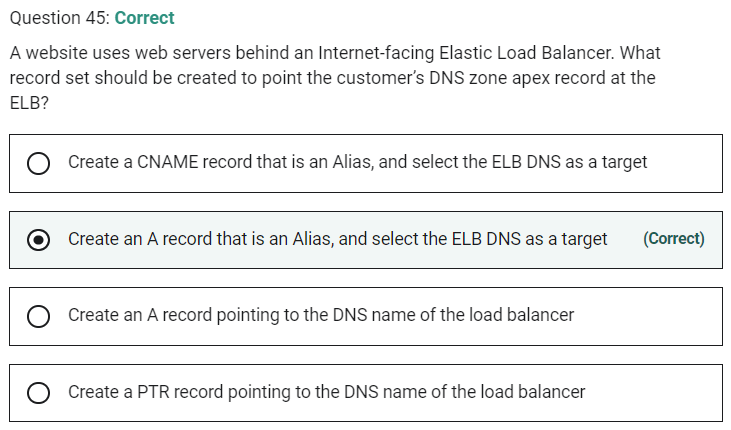
**INCORRECT:** "Configure an IPSec VPN connection over the Direct Connect link" is incorrect. This is not a solution to the problem as the VPN connection is going over the Direct Connect link. This is something you might do to add encryption to Direct Connect but it doesn’t make it more resilient.

Marked

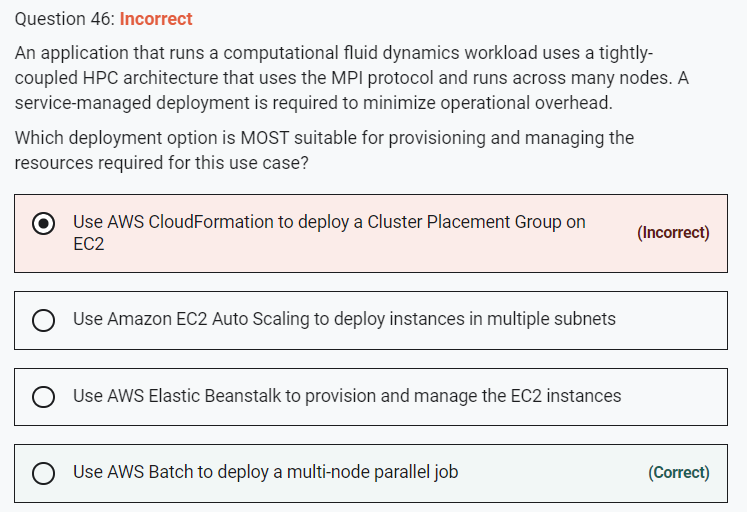


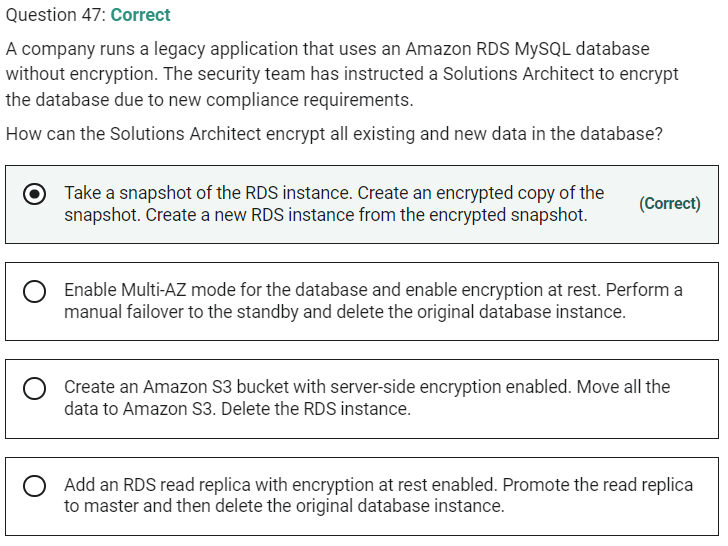
Marked

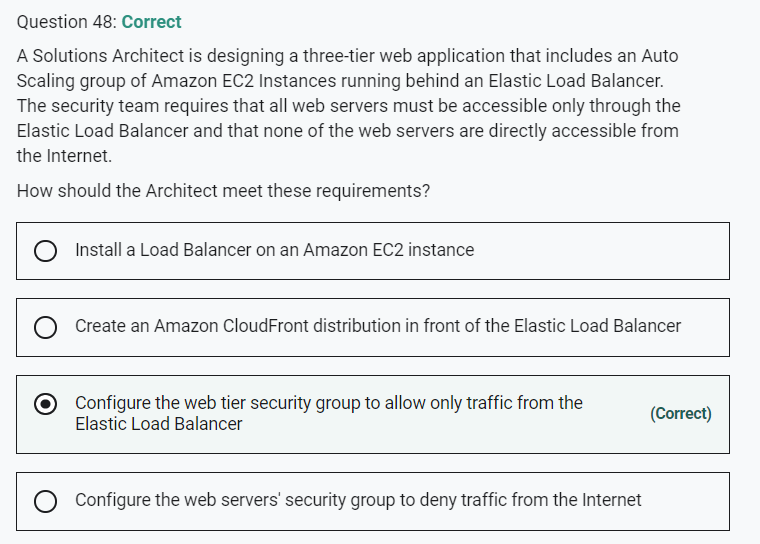




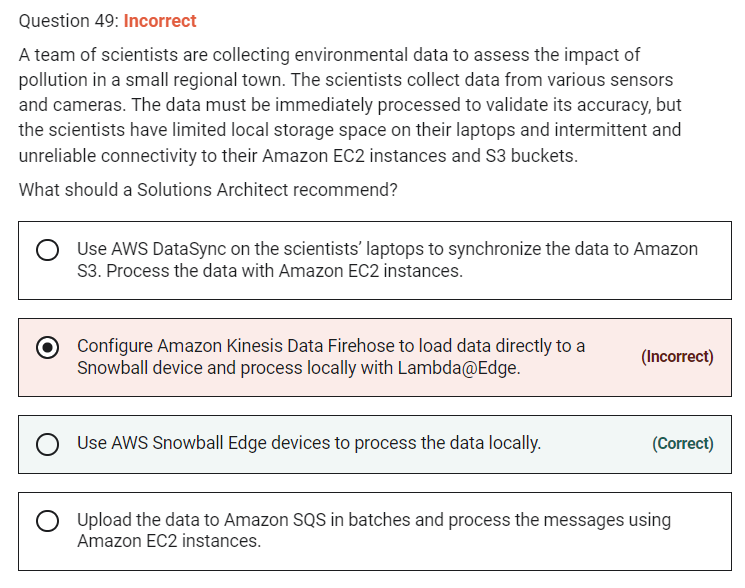
Marked

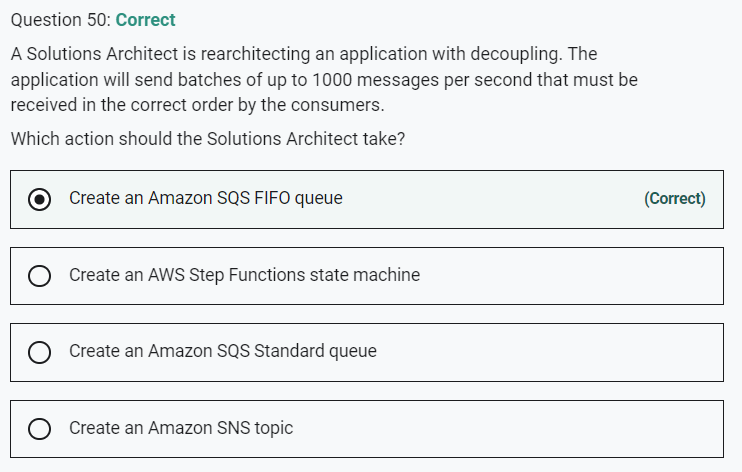




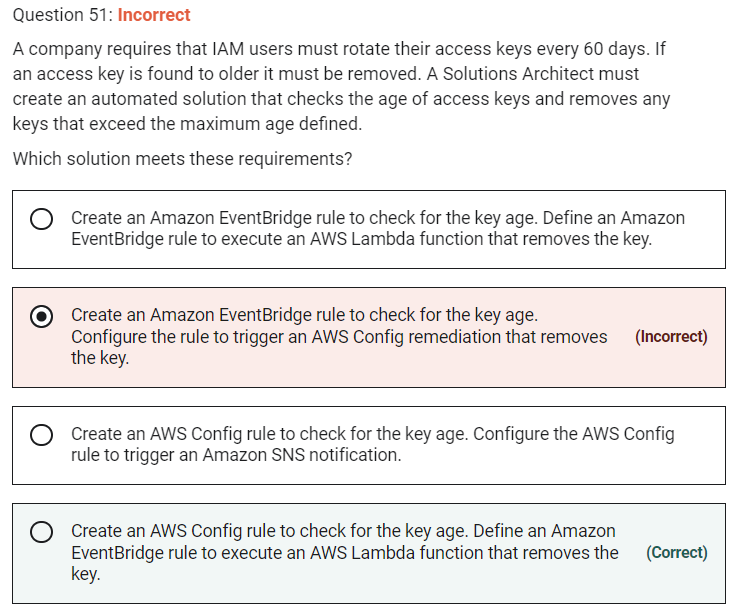


Marked

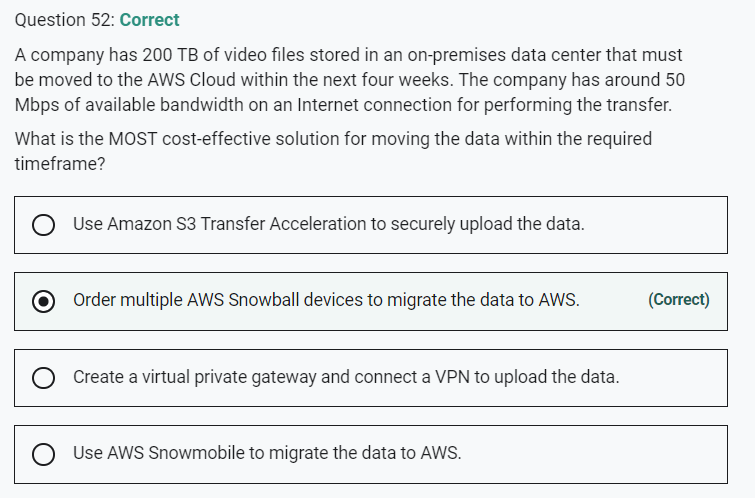




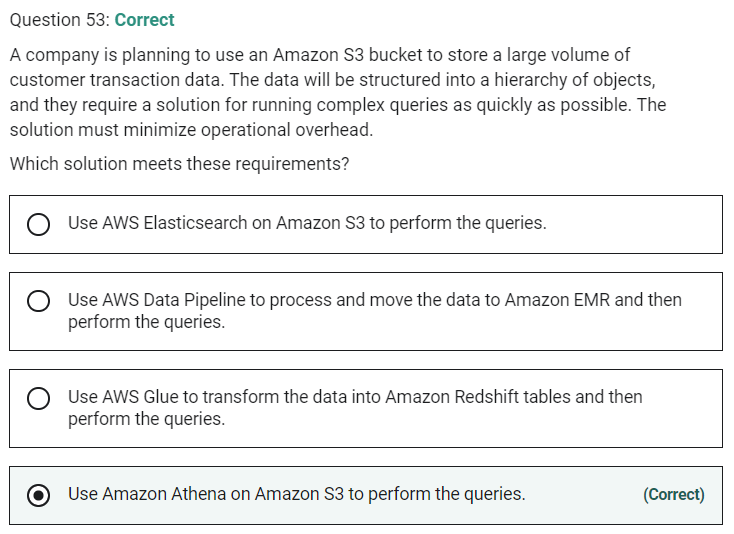
Marked

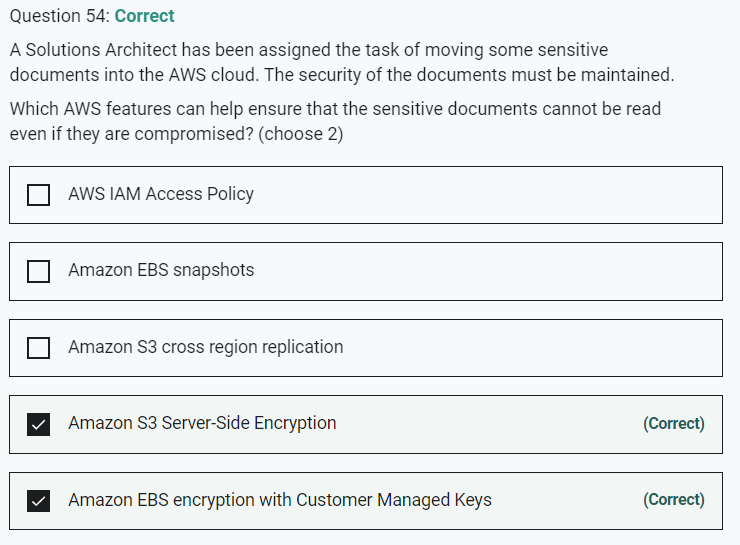


Marked

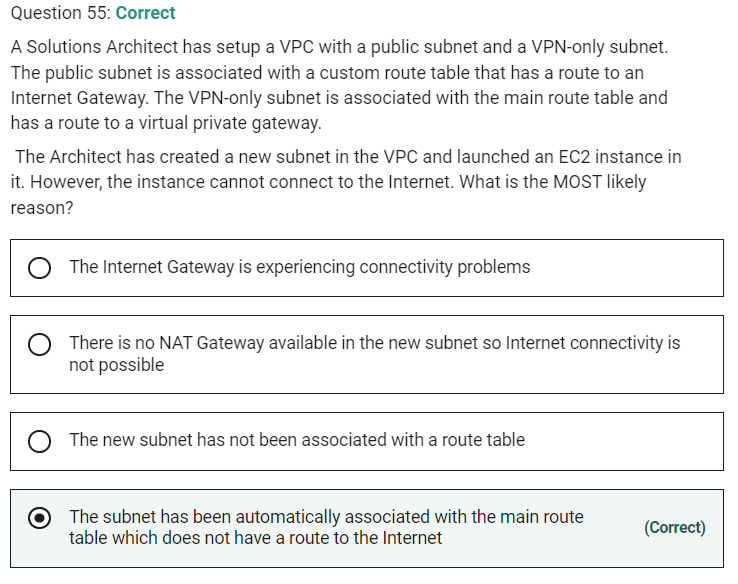


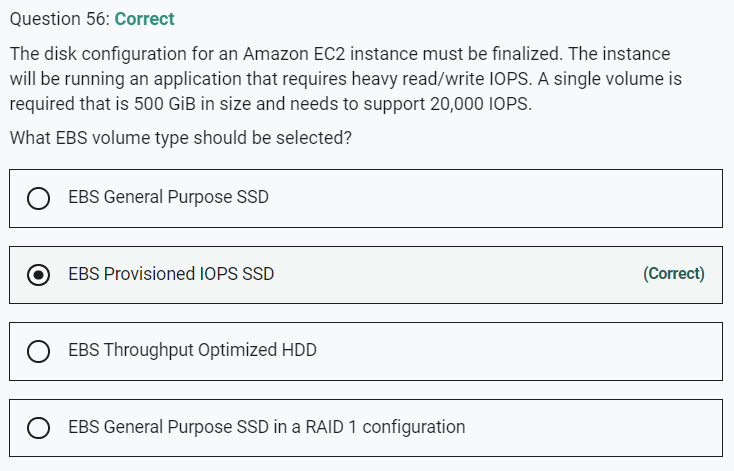
**INCORRECT:** "Use AWS Snowmobile to migrate the data to AWS" is incorrect. This is a very large device on the back of a truck that is used for moving huge quantities of data. It would be very expensive for moving just 200 TB of data.



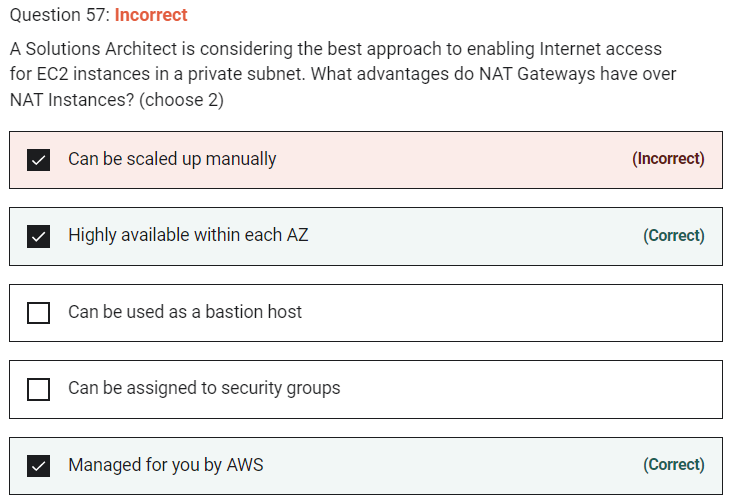


Marked



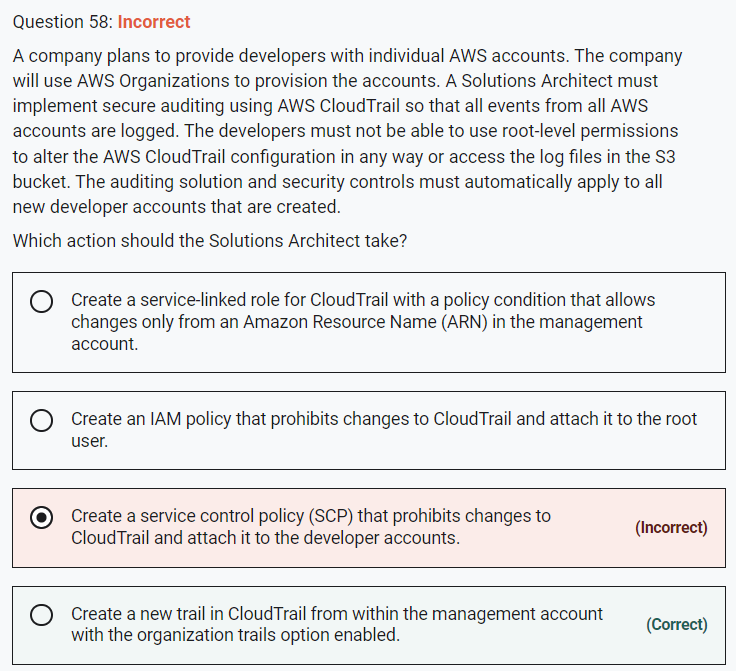


Marked

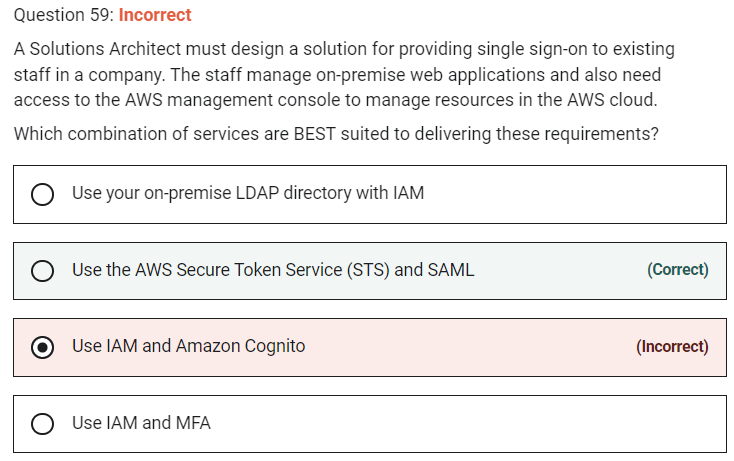


NAT gateways are highly available in each AZ into which they are deployed. They are not associated with any security groups and can scale automatically up to 45Gbps

Marked



Marked



Single sign-on using federation allows users to login to the AWS console without assigning IAM credentials. The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for IAM users or for users that you authenticate (such as federated users from an on-premise directory).

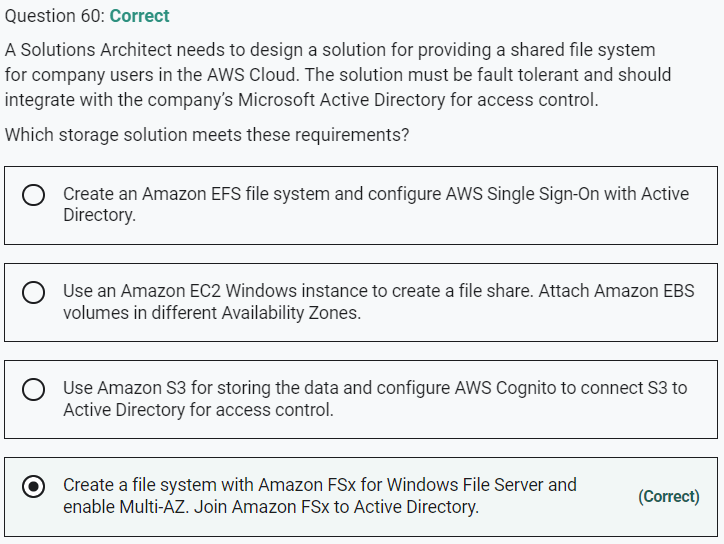
Federation (typically Active Directory) uses SAML 2.0 for authentication and grants temporary access based on the users AD credentials. The user does not need to be a user in IAM.

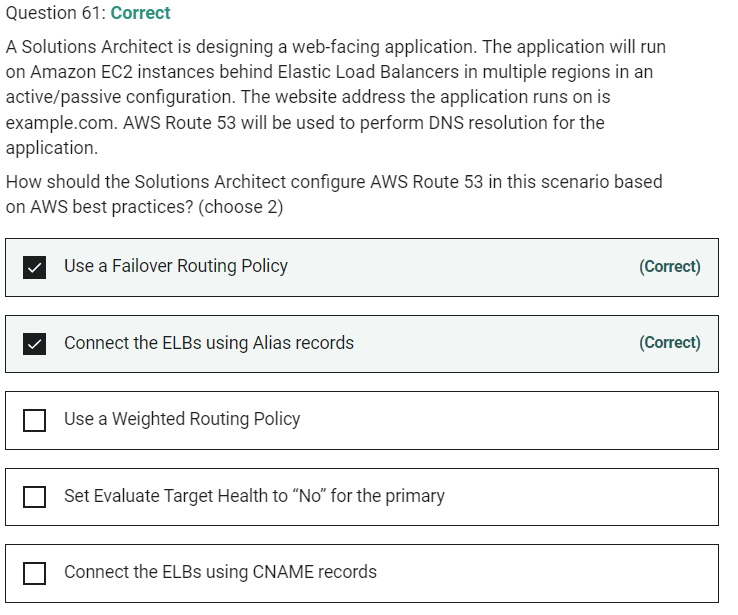
**CORRECT:**"Use the AWS Secure Token Service (STS) and SAML" is the correct answer.

**INCORRECT:** "Use IAM and Amazon Cognito" is incorrect. Amazon Cognito is used for authenticating users to web and mobile apps not for providing single sign-on between on-premises directories and the AWS management console.

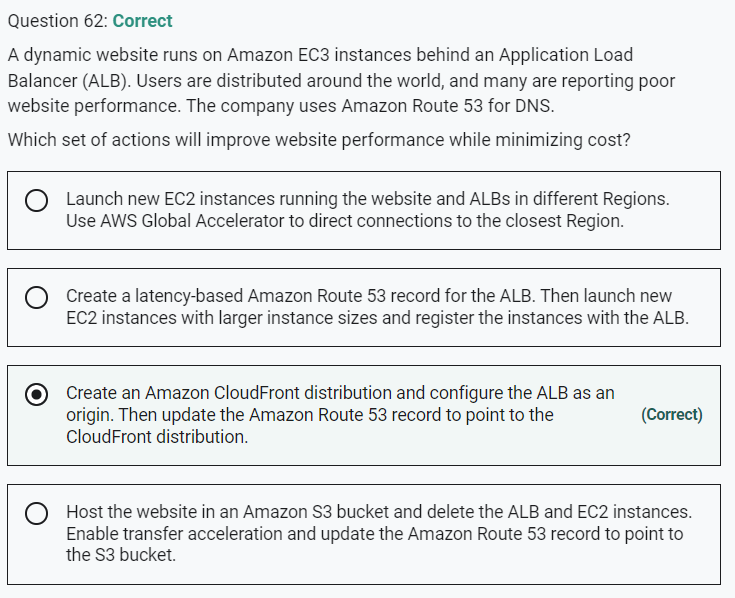
**INCORRECT:** "Use your on-premise LDAP directory with IAM" is incorrect. You cannot use your on-premise LDAP directory with IAM, you must use federation.

**INCORRECT:** "Use IAM and MFA" is incorrect. Enabling multi-factor authentication (MFA) for IAM is not a federation solution..

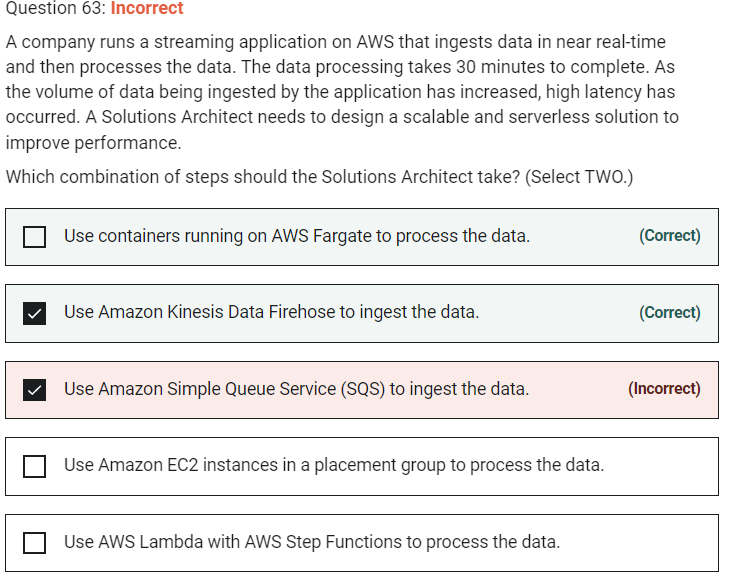


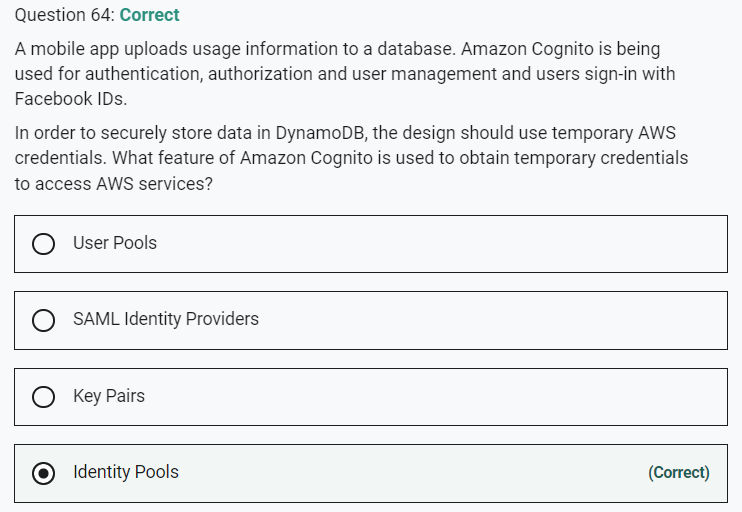


Marked



Marked





Marked

