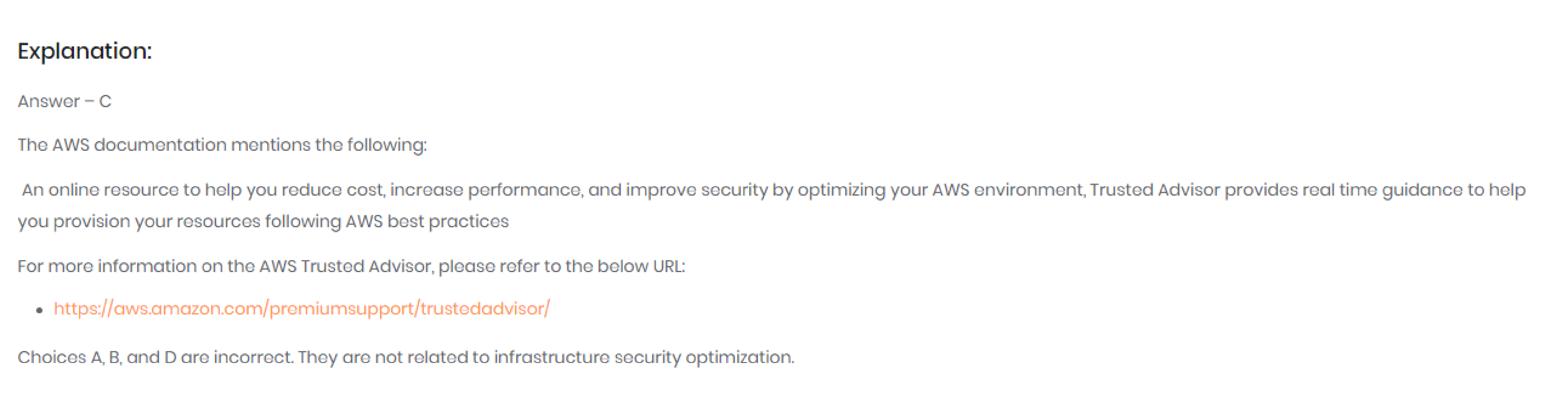
Final Assessment 1 Answer & Explanation

Date 19-jan-22

CONTINUE TO
Next Slide

Ques No : 01



Explanation:

Answer – C

The AWS documentation mentions the following:

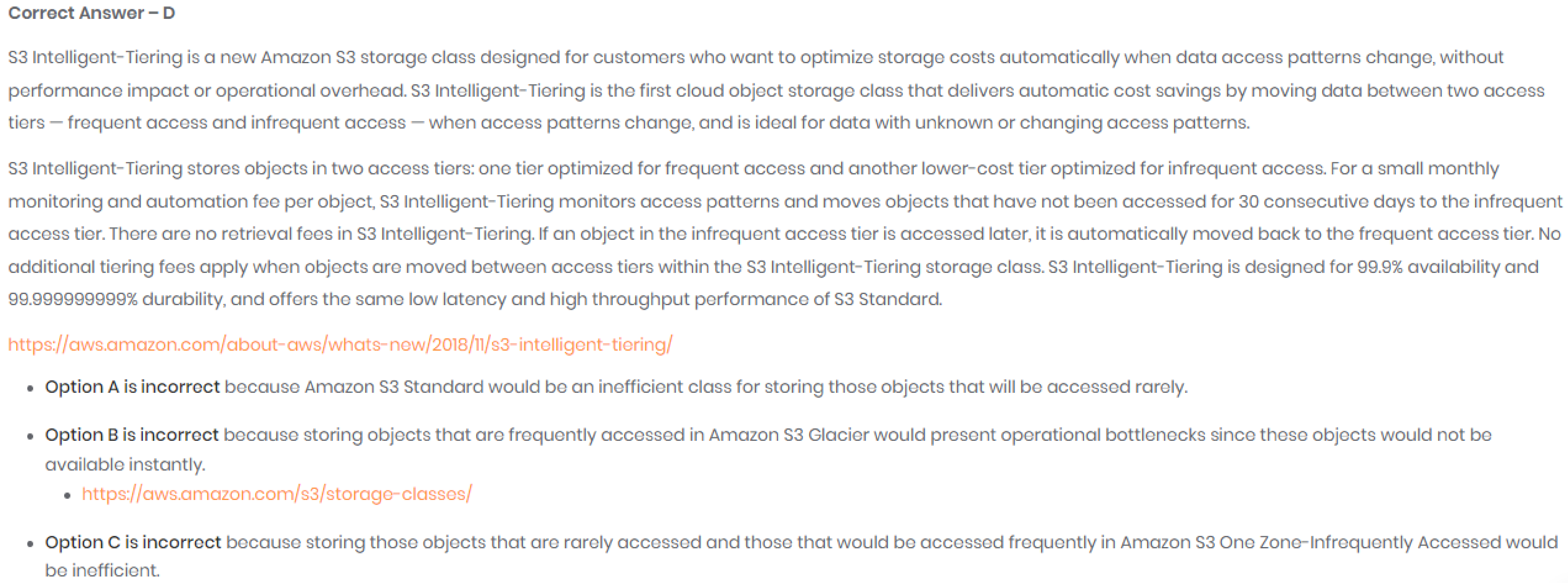
An online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment, Trusted Advisor provides real time guidance to help you provision your resources following AWS best practices

For more information on the AWS Trusted Advisor, please refer to the below URL:

- https://aws.amazon.com/premiumsupport/trustedadvisor/

Choices A, B, and D are incorrect. They are not related to infrastructure security optimization.

Ques No : 02



Correct Answer – D

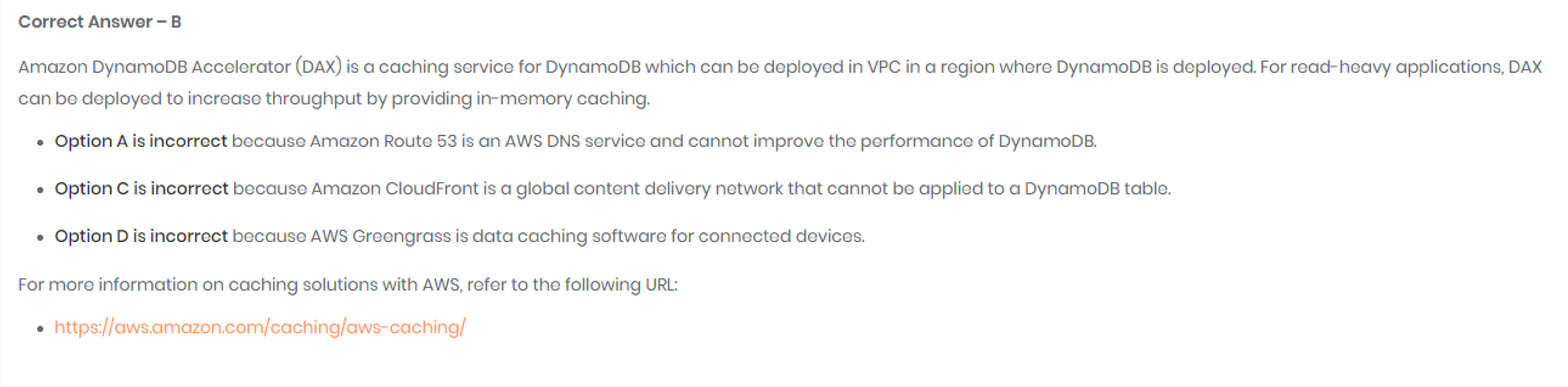
S3 Intelligent-Tiering is a new Amazon S3 storage class designed for customers who want to optimize storage costs automatically when data access patterns change, without performance impact or operational overhead. S3 Intelligent-Tiering is the first cloud object storage class that delivers automatic cost savings by moving data between two access tiers — frequent access and infrequent access — when access patterns change, and is ideal for data with unknown or changing access patterns.

S3 Intelligent-Tiering stores objects in two access tiers: one tier optimized for frequent access and another lower-cost tier optimized for infrequent access. For a small monthly monitoring and automation fee per object, S3 Intelligent-Tiering monitors access patterns and moves objects that have not been accessed for 30 consecutive days to the infrequent access tier. There are no retrieval fees in S3 Intelligent-Tiering. If an object in the infrequent access tier is accessed later, it is automatically moved back to the frequent access tier. No additional tiering fees apply when objects are moved between access tiers within the S3 Intelligent-Tiering storage class. S3 Intelligent-Tiering is designed for 99.9% availability and 99.999999999% durability, and offers the same low latency and high throughput performance of S3 Standard.

https://aws.amazon.com/about-aws/whats-new/2018/11/s3-intelligent-tiering/

- **Option A is incorrect** because Amazon S3 Standard would be an inefficient class for storing those objects that will be accessed rarely.
- **Option B is incorrect** because storing objects that are frequently accessed in Amazon S3 Glacier would present operational bottlenecks since these objects would not be available instantly.
  - https://aws.amazon.com/s3/storage-classes/
- **Option C is incorrect** because storing those objects that are rarely accessed and those that would be accessed frequently in Amazon S3 One Zone-Infrequently Accessed would be inefficient.

Ques No : 03



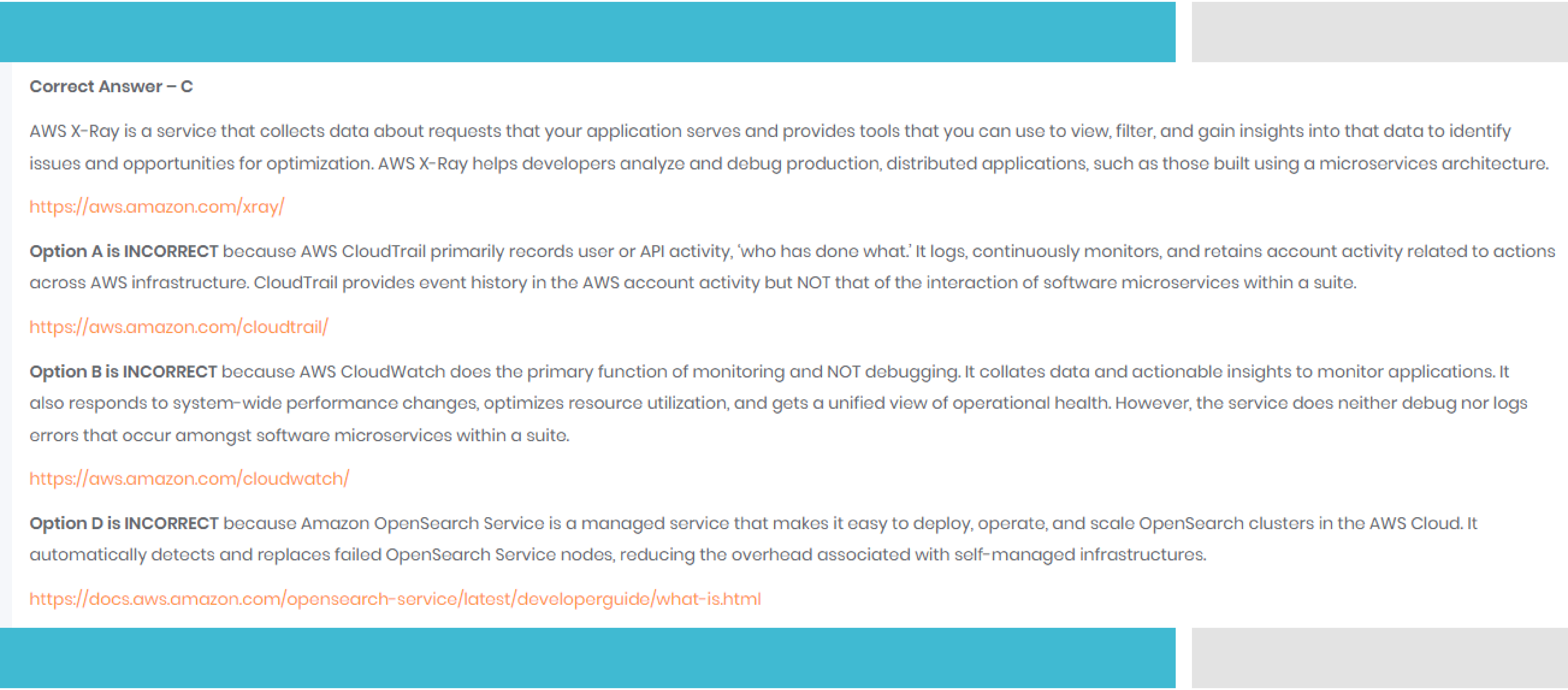
Correct Answer – B

Amazon DynamoDB Accelerator (DAX) is a caching service for DynamoDB which can be deployed in VPC in a region where DynamoDB is deployed. For read-heavy applications, DAX can be deployed to increase throughput by providing in-memory caching.

- **Option A is incorrect** because Amazon Route 53 is an AWS DNS service and cannot improve the performance of DynamoDB.
- **Option C is incorrect** because Amazon CloudFront is a global content delivery network that cannot be applied to a DynamoDB table.
- **Option D is incorrect** because AWS Greengrass is data caching software for connected devices.

For more information on caching solutions with AWS, refer to the following URL:

- https://aws.amazon.com/caching/aws-caching/



Correct Answer – C

AWS X-Ray is a service that collects data about requests that your application serves and provides tools that you can use to view, filter, and gain insights into that data to identify issues and opportunities for optimization. AWS X-Ray helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture.

https://aws.amazon.com/xray/

Option A is INCORRECT because AWS CloudTrail primarily records user or API activity, 'who has done what.' It logs, continuously monitors, and retains account activity related to actions across AWS infrastructure. CloudTrail provides event history in the AWS account activity but NOT that of the interaction of software microservices within a suite.

https://aws.amazon.com/cloudtrail/

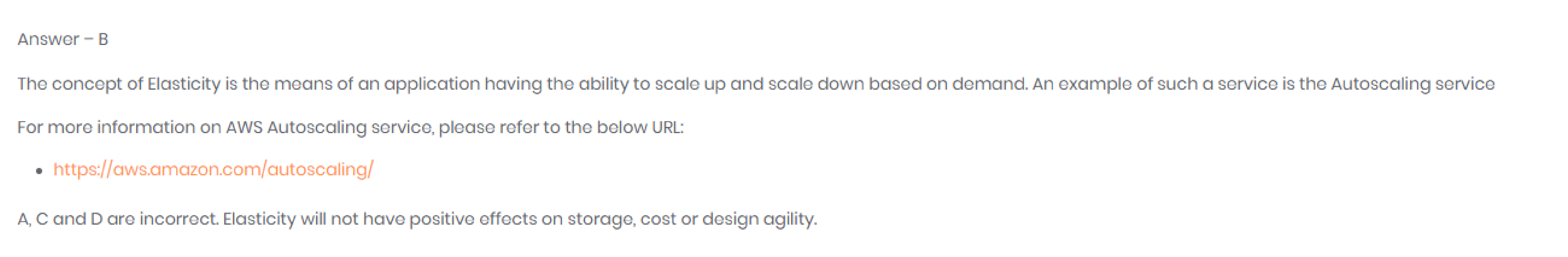
Option B is INCORRECT because AWS CloudWatch does the primary function of monitoring and NOT debugging. It collates data and actionable insights to monitor applications. It also responds to system-wide performance changes, optimizes resource utilization, and gets a unified view of operational health. However, the service does neither debug nor logs errors that occur amongst software microservices within a suite.

https://aws.amazon.com/cloudwatch/

Option D is INCORRECT because Amazon OpenSearch Service is a managed service that makes it easy to deploy, operate, and scale OpenSearch clusters in the AWS Cloud. It automatically detects and replaces failed OpenSearch Service nodes, reducing the overhead associated with self-managed infrastructures.

https://docs.aws.amazon.com/opensearch-service/latest/developerguide/what-is.html

Ques No : 05



Answer – B

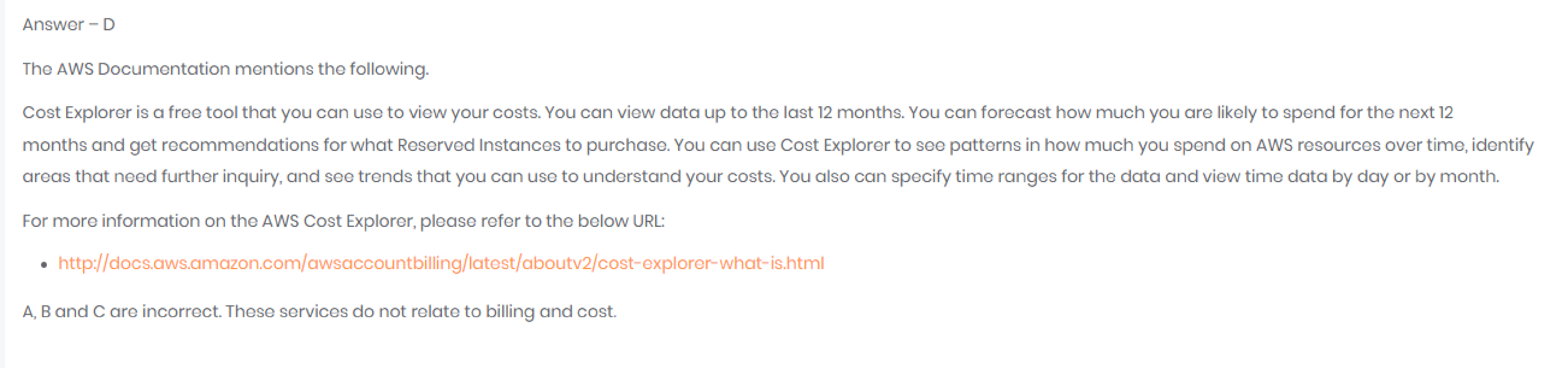
The concept of Elasticity is the means of an application having the ability to scale up and scale down based on demand. An example of such a service is the Autoscaling service

For more information on AWS Autoscaling service, please refer to the below URL:

- https://aws.amazon.com/autoscaling/

A, C and D are incorrect. Elasticity will not have positive effects on storage, cost or design agility.

Ques No : 06



Answer – D

The AWS Documentation mentions the following.

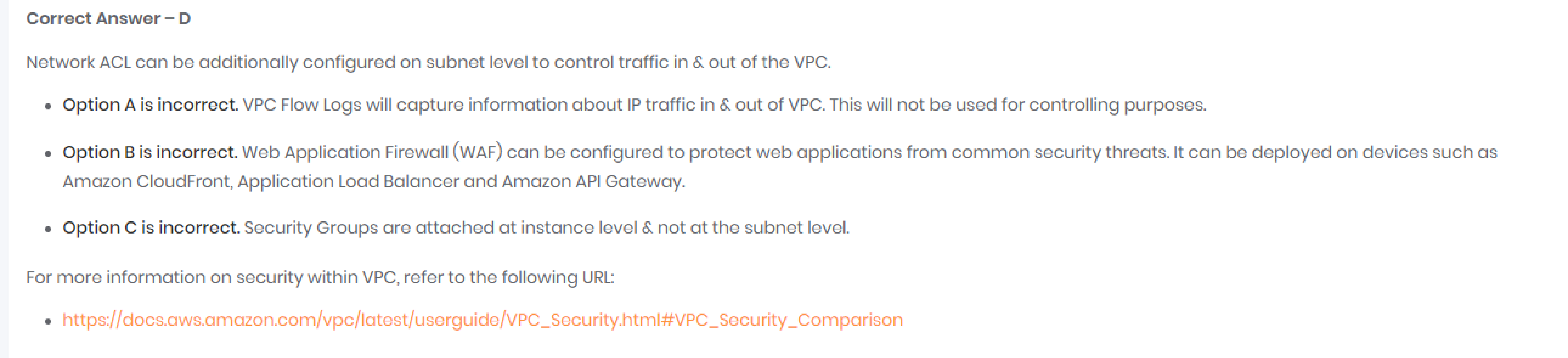
Cost Explorer is a free tool that you can use to view your costs. You can view data up to the last 12 months. You can forecast how much you are likely to spend for the next 12 months and get recommendations for what Reserved Instances to purchase. You can use Cost Explorer to see patterns in how much you spend on AWS resources over time, identify areas that need further inquiry, and see trends that you can use to understand your costs. You also can specify time ranges for the data and view time data by day or by month.

For more information on the AWS Cost Explorer, please refer to the below URL:

- http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/cost-explorer-what-is.html

A, B and C are incorrect. These services do not relate to billing and cost.

Ques No : 07



Correct Answer – D

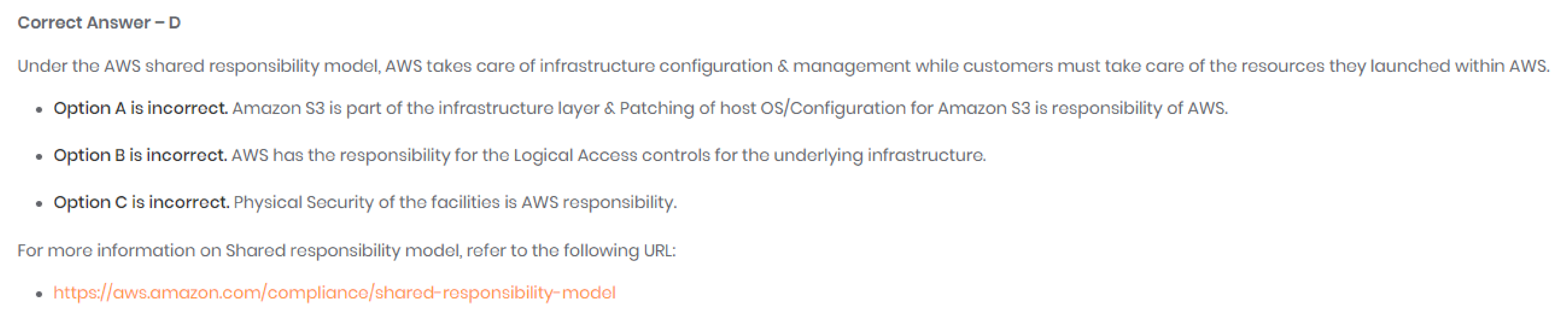
Network ACL can be additionally configured on subnet level to control traffic in & out of the VPC.

- **Option A is incorrect.** VPC Flow Logs will capture information about IP traffic in & out of VPC. This will not be used for controlling purposes.
- **Option B is incorrect.** Web Application Firewall (WAF) can be configured to protect web applications from common security threats. It can be deployed on devices such as Amazon CloudFront, Application Load Balancer and Amazon API Gateway.
- **Option C is incorrect.** Security Groups are attached at instance level & not at the subnet level.

For more information on security within VPC, refer to the following URL:

- https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html#VPC_Security_Comparison

Ques No : 08



Correct Answer – D

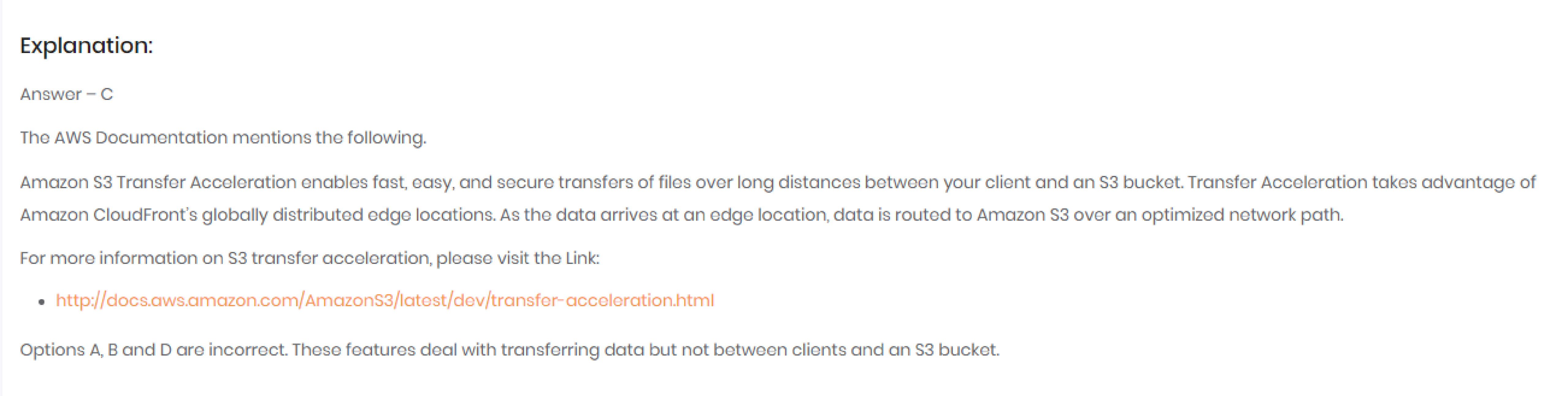
Under the AWS shared responsibility model, AWS takes care of infrastructure configuration & management while customers must take care of the resources they launched within AWS.

- **Option A is incorrect.** Amazon S3 is part of the infrastructure layer & Patching of host OS/Configuration for Amazon S3 is responsibility of AWS.
- **Option B is incorrect.** AWS has the responsibility for the Logical Access controls for the underlying infrastructure.
- **Option C is incorrect.** Physical Security of the facilities is AWS responsibility.

For more information on Shared responsibility model, refer to the following URL:

- https://aws.amazon.com/compliance/shared-responsibility-model

Ques No : 09



Explanation:

Answer – C

The AWS Documentation mentions the following.

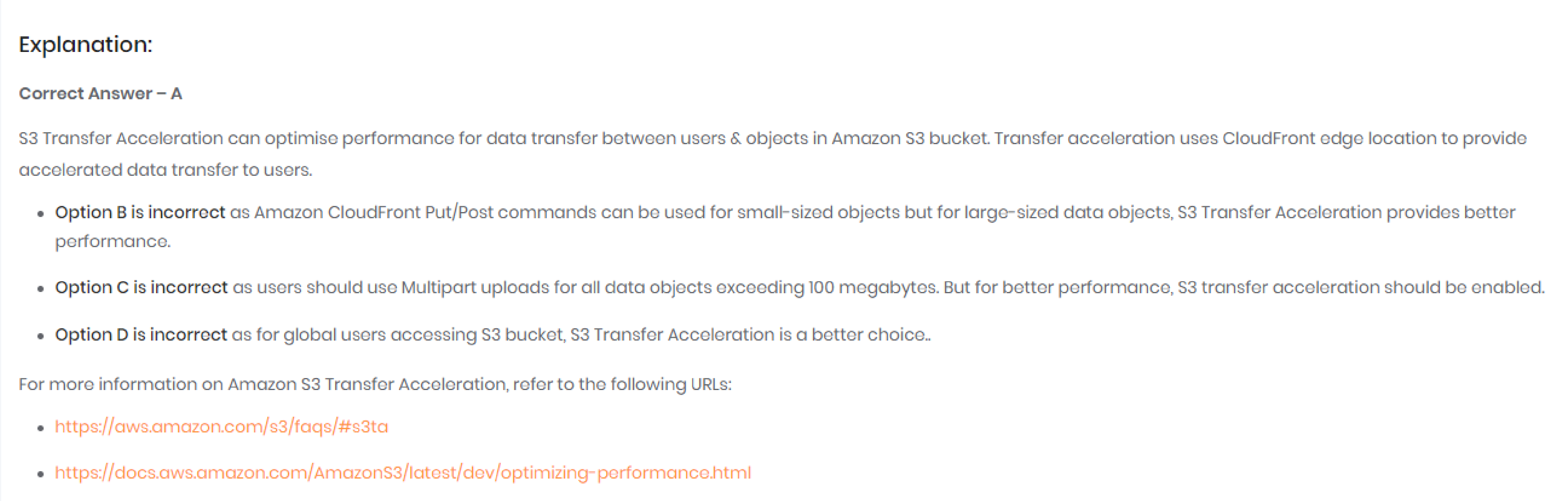
Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration takes advantage of Amazon CloudFront's globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path.

For more information on S3 transfer acceleration, please visit the Link:

- http://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html

Options A, B and D are incorrect. These features deal with transferring data but not between clients and an S3 bucket.

Ques No : 10



Explanation:

Correct Answer – A

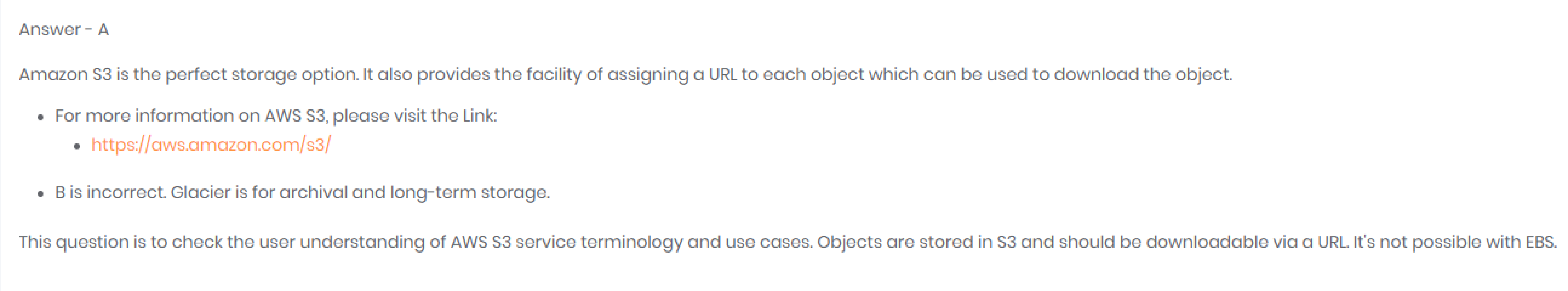
S3 Transfer Acceleration can optimise performance for data transfer between users & objects in Amazon S3 bucket. Transfer acceleration uses CloudFront edge location to provide accelerated data transfer to users.

- **Option B is incorrect** as Amazon CloudFront Put/Post commands can be used for small-sized objects but for large-sized data objects, S3 Transfer Acceleration provides better performance.
- **Option C is incorrect** as users should use Multipart uploads for all data objects exceeding 100 megabytes. But for better performance, S3 transfer acceleration should be enabled.
- **Option D is incorrect** as for global users accessing S3 bucket, S3 Transfer Acceleration is a better choice..

For more information on Amazon S3 Transfer Acceleration, refer to the following URLs:

- https://aws.amazon.com/s3/faqs/#s3ta
- https://docs.aws.amazon.com/AmazonS3/latest/dev/optimizing-performance.html

Ques No : 11



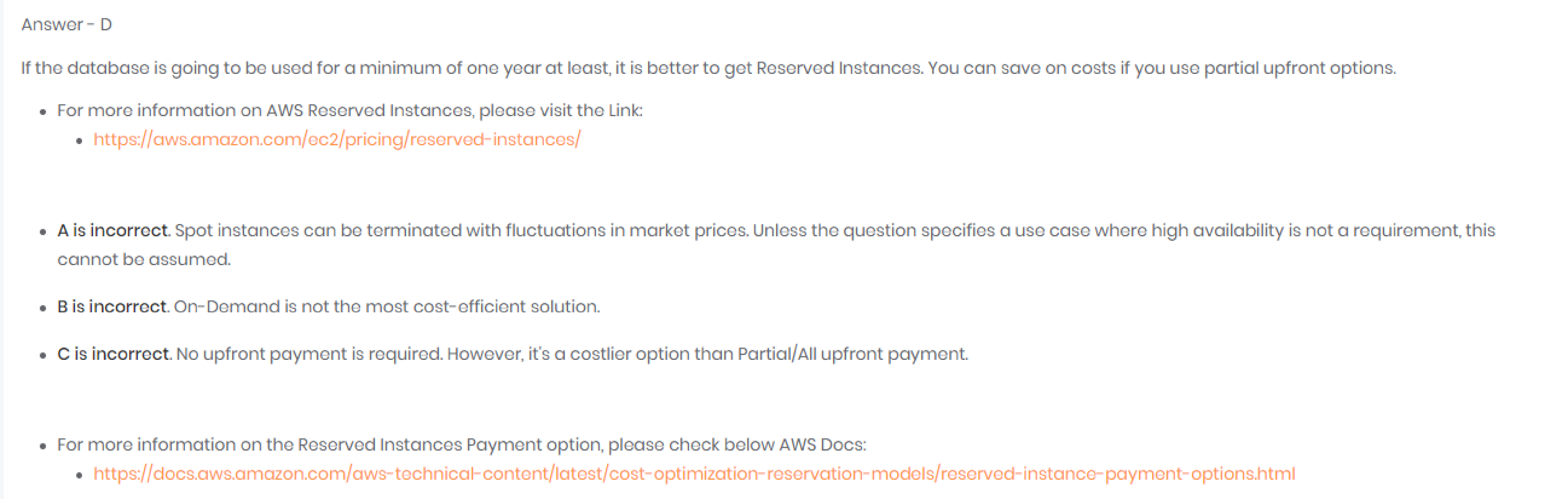
Answer - A

Amazon S3 is the perfect storage option. It also provides the facility of assigning a URL to each object which can be used to download the object.

- For more information on AWS S3, please visit the Link:
  - https://aws.amazon.com/s3/
- B is incorrect. Glacier is for archival and long-term storage.

This question is to check the user understanding of AWS S3 service terminology and use cases. Objects are stored in S3 and should be downloadable via a URL. It's not possible with EBS.

Ques No : 12



Answer - D

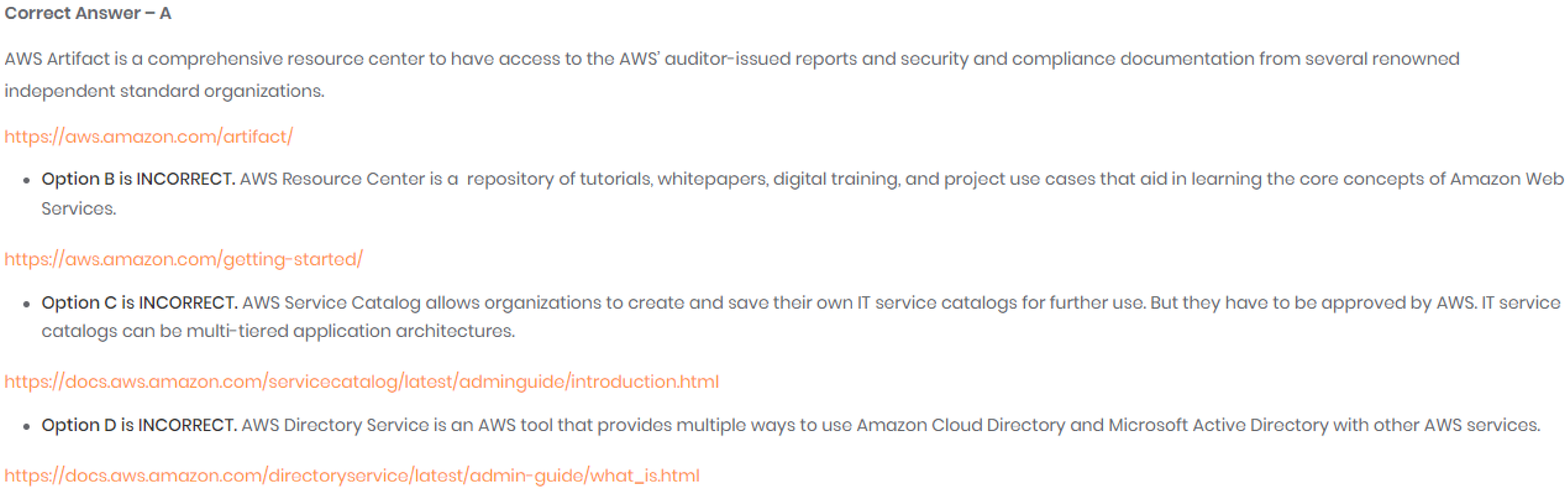
If the database is going to be used for a minimum of one year at least, it is better to get Reserved Instances. You can save on costs if you use partial upfront options.

- For more information on AWS Reserved Instances, please visit the Link:
  - https://aws.amazon.com/ec2/pricing/reserved-instances/

- **A is incorrect**. Spot instances can be terminated with fluctuations in market prices. Unless the question specifies a use case where high availability is not a requirement, this cannot be assumed.
- **B is incorrect**. On-Demand is not the most cost-efficient solution.
- **C is incorrect**. No upfront payment is required. However, it's a costlier option than Partial/All upfront payment.

- For more information on the Reserved Instances Payment option, please check below AWS Docs:
  - https://docs.aws.amazon.com/aws-technical-content/latest/cost-optimization-reservation-models/reserved-instance-payment-options.html

Ques No : 13



Correct Answer – A

AWS Artifact is a comprehensive resource center to have access to the AWS' auditor-issued reports and security and compliance documentation from several renowned independent standard organizations.

https://aws.amazon.com/artifact/

- **Option B is INCORRECT.** AWS Resource Center is a repository of tutorials, whitepapers, digital training, and project use cases that aid in learning the core concepts of Amazon Web Services.

https://aws.amazon.com/getting-started/

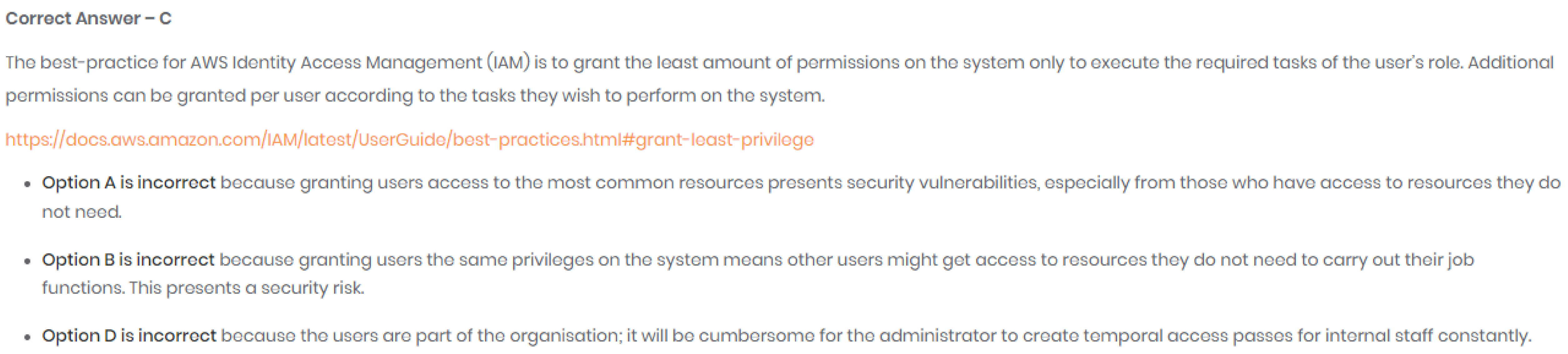
- **Option C is INCORRECT.** AWS Service Catalog allows organizations to create and save their own IT service catalogs for further use. But they have to be approved by AWS. IT service catalogs can be multi-tiered application architectures.

https://docs.aws.amazon.com/servicecatalog/latest/adminguide/introduction.html

- **Option D is INCORRECT.** AWS Directory Service is an AWS tool that provides multiple ways to use Amazon Cloud Directory and Microsoft Active Directory with other AWS services.

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html

Ques No : 14



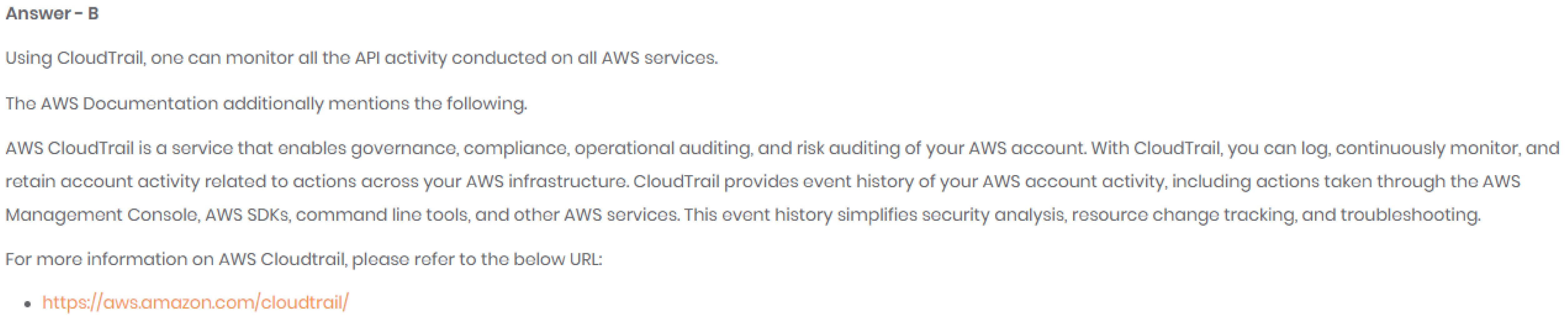
Correct Answer – C

The best-practice for AWS Identity Access Management (IAM) is to grant the least amount of permissions on the system only to execute the required tasks of the user's role. Additional permissions can be granted per user according to the tasks they wish to perform on the system.

https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege

- **Option A is incorrect** because granting users access to the most common resources presents security vulnerabilities, especially from those who have access to resources they do not need.
- **Option B is incorrect** because granting users the same privileges on the system means other users might get access to resources they do not need to carry out their job functions. This presents a security risk.
- **Option D is incorrect** because the users are part of the organisation; it will be cumbersome for the administrator to create temporal access passes for internal staff constantly.

Ques No : 15



Answer - B

Using CloudTrail, one can monitor all the API activity conducted on all AWS services.

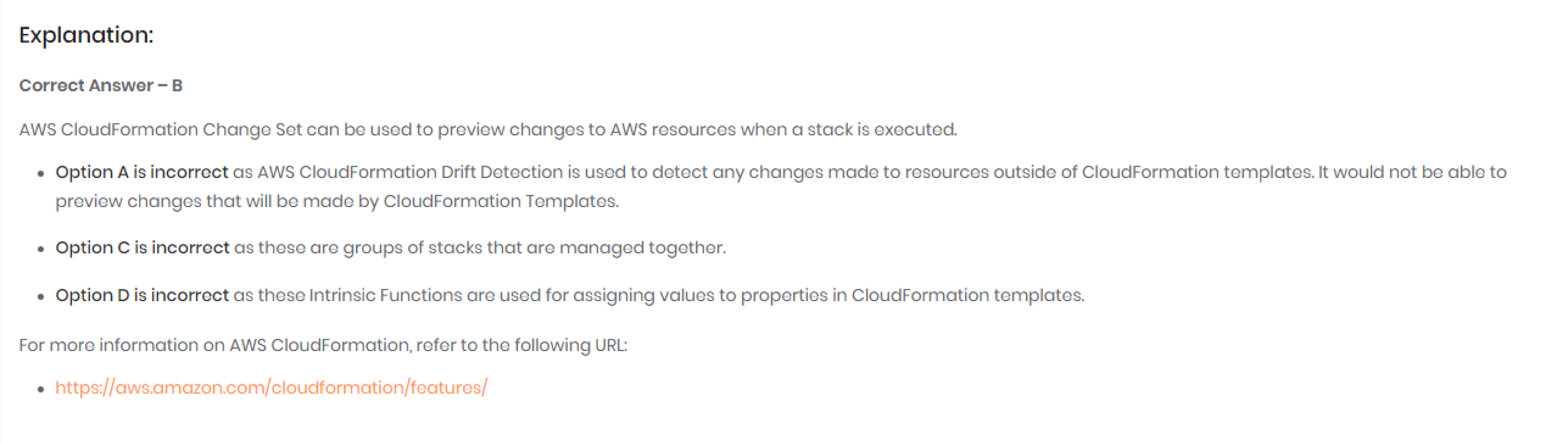
The AWS Documentation additionally mentions the following.

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.

For more information on AWS Cloudtrail, please refer to the below URL:

- https://aws.amazon.com/cloudtrail/

Ques No : 016



Explanation:

Correct Answer – B

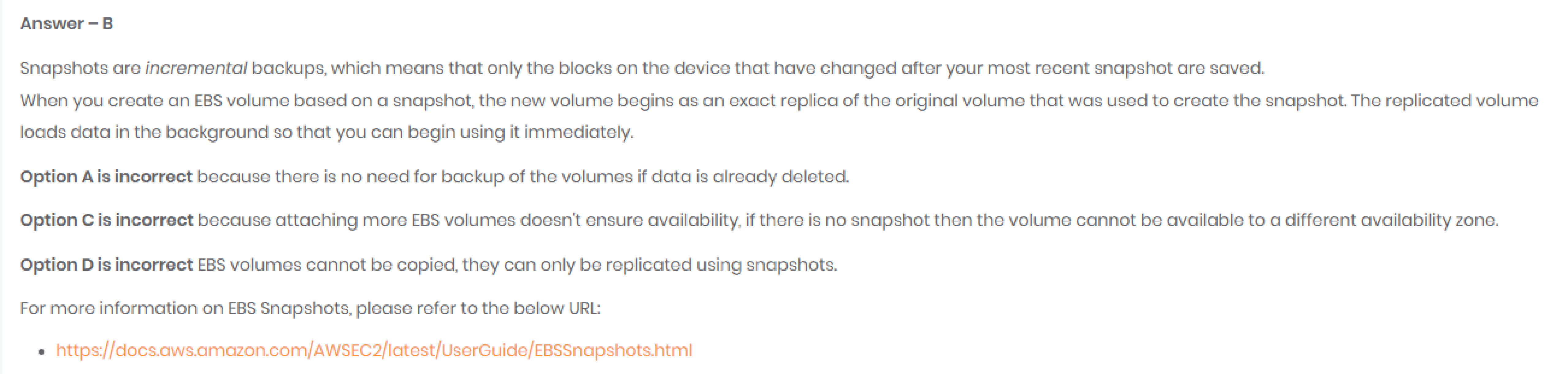
AWS CloudFormation Change Set can be used to preview changes to AWS resources when a stack is executed.

- **Option A is incorrect** as AWS CloudFormation Drift Detection is used to detect any changes made to resources outside of CloudFormation templates. It would not be able to preview changes that will be made by CloudFormation Templates.
- **Option C is incorrect** as these are groups of stacks that are managed together.
- **Option D is incorrect** as these Intrinsic Functions are used for assigning values to properties in CloudFormation templates.

For more information on AWS CloudFormation, refer to the following URL:

- https://aws.amazon.com/cloudformation/features/

Ques No : 17



Answer – B

Snapshots are *incremental* backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved.
When you create an EBS volume based on a snapshot, the new volume begins as an exact replica of the original volume that was used to create the snapshot. The replicated volume loads data in the background so that you can begin using it immediately.

Option A is incorrect because there is no need for backup of the volumes if data is already deleted.

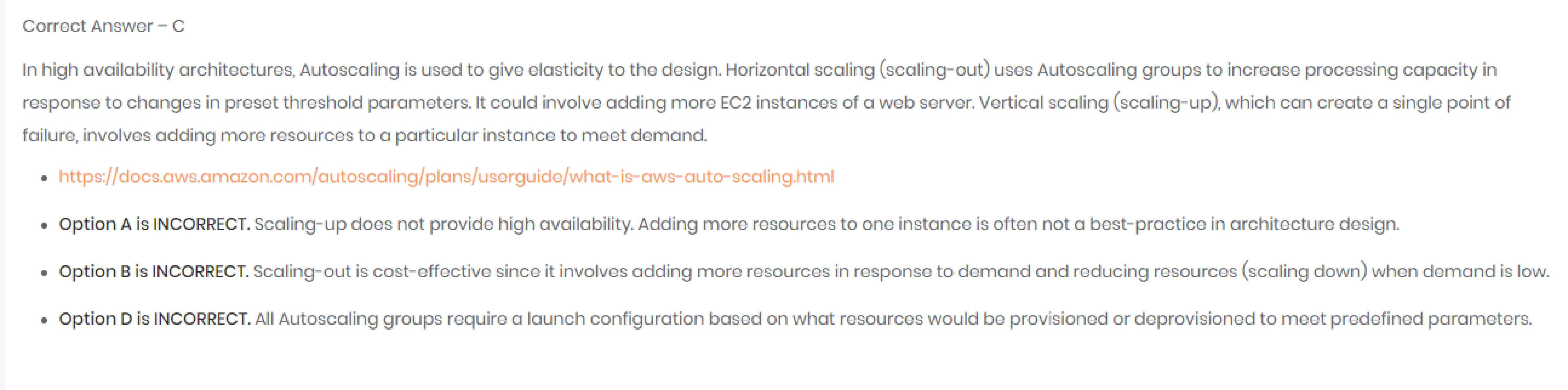
Option C is incorrect because attaching more EBS volumes doesn't ensure availability, if there is no snapshot then the volume cannot be available to a different availability zone.

Option D is incorrect EBS volumes cannot be copied, they can only be replicated using snapshots.

For more information on EBS Snapshots, please refer to the below URL:

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html

Ques No : 18

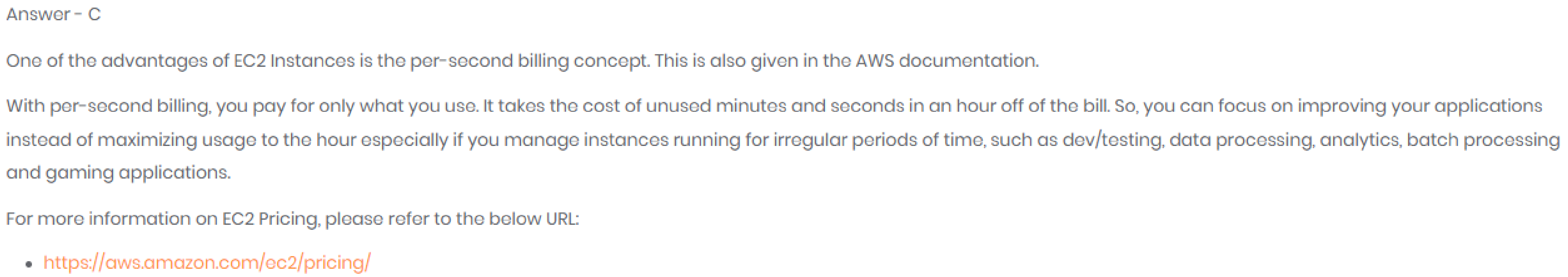


Correct Answer – C

In high availability architectures, Autoscaling is used to give elasticity to the design. Horizontal scaling (scaling-out) uses Autoscaling groups to increase processing capacity in response to changes in preset threshold parameters. It could involve adding more EC2 instances of a web server. Vertical scaling (scaling-up), which can create a single point of failure, involves adding more resources to a particular instance to meet demand.

- https://docs.aws.amazon.com/autoscaling/plans/userguide/what-is-aws-auto-scaling.html
- **Option A is INCORRECT.** Scaling-up does not provide high availability. Adding more resources to one instance is often not a best-practice in architecture design.
- **Option B is INCORRECT.** Scaling-out is cost-effective since it involves adding more resources in response to demand and reducing resources (scaling down) when demand is low.
- **Option D is INCORRECT.** All Autoscaling groups require a launch configuration based on what resources would be provisioned or deprovisioned to meet predefined parameters.

Ques No : 19



Answer - C

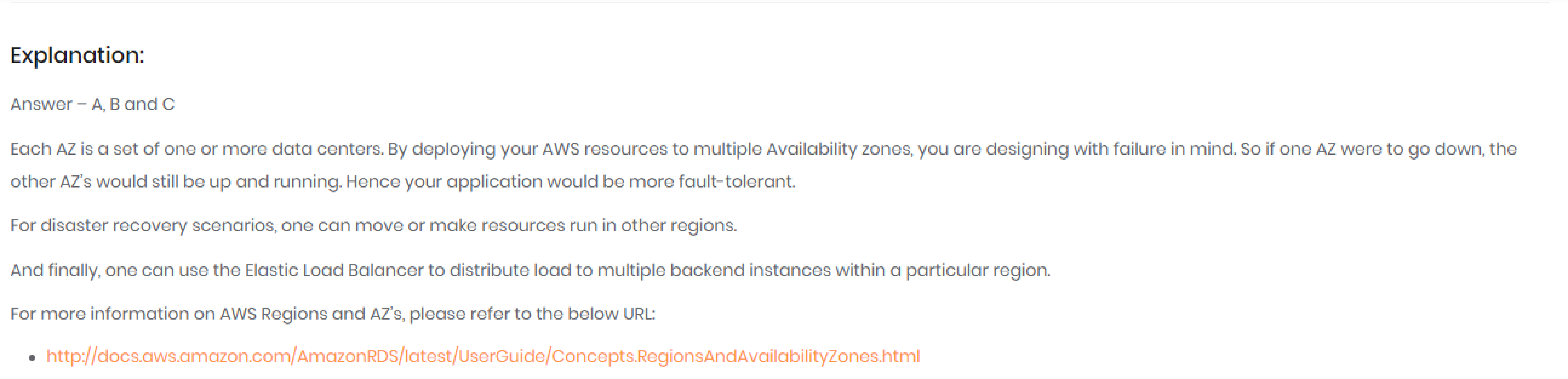
One of the advantages of EC2 Instances is the per-second billing concept. This is also given in the AWS documentation.

With per-second billing, you pay for only what you use. It takes the cost of unused minutes and seconds in an hour off of the bill. So, you can focus on improving your applications instead of maximizing usage to the hour especially if you manage instances running for irregular periods of time, such as dev/testing, data processing, analytics, batch processing and gaming applications.

For more information on EC2 Pricing, please refer to the below URL:

- https://aws.amazon.com/ec2/pricing/

Ques No : 20



Explanation:

Answer – A, B and C

Each AZ is a set of one or more data centers. By deploying your AWS resources to multiple Availability zones, you are designing with failure in mind. So if one AZ were to go down, the other AZ's would still be up and running. Hence your application would be more fault-tolerant.

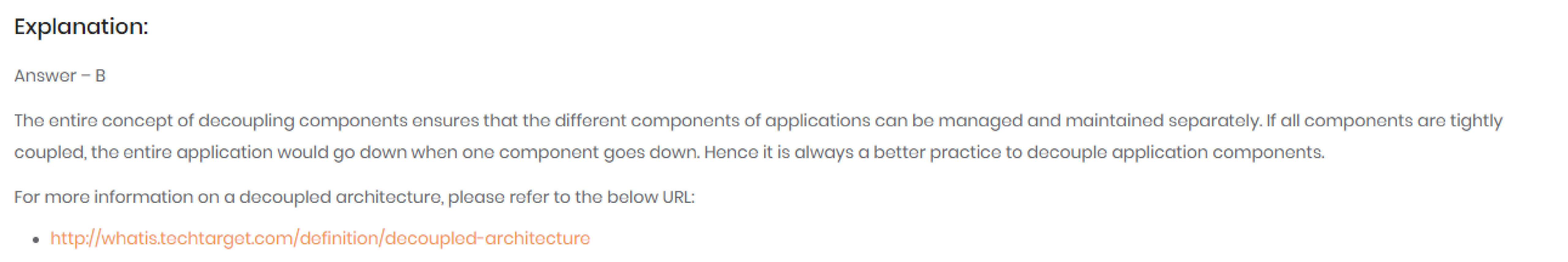
For disaster recovery scenarios, one can move or make resources run in other regions.

And finally, one can use the Elastic Load Balancer to distribute load to multiple backend instances within a particular region.

For more information on AWS Regions and AZ's, please refer to the below URL:

- http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RegionsAndAvailabilityZones.html

Ques No : 21



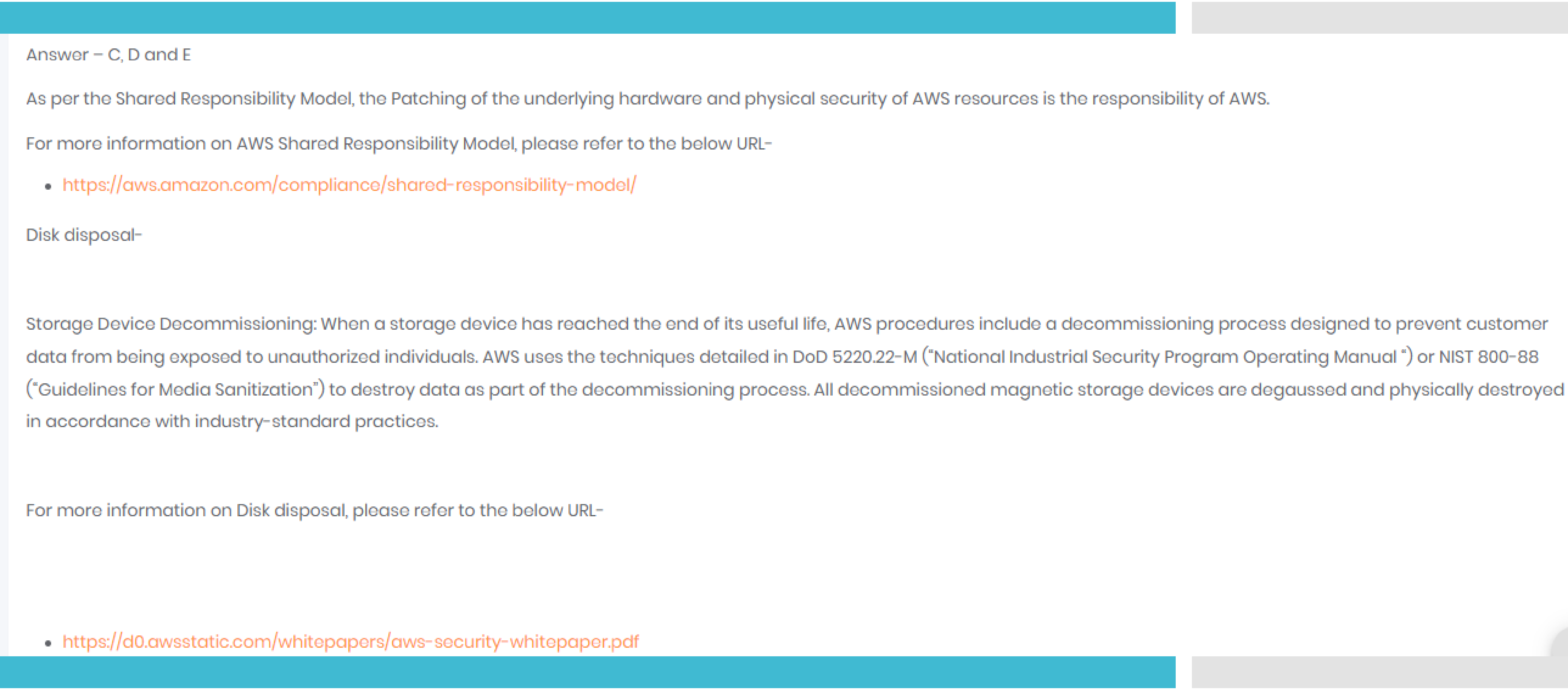
Explanation:

Answer – B

The entire concept of decoupling components ensures that the different components of applications can be managed and maintained separately. If all components are tightly coupled, the entire application would go down when one component goes down. Hence it is always a better practice to decouple application components.

For more information on a decoupled architecture, please refer to the below URL:

- http://whatis.techtarget.com/definition/decoupled-architecture



Answer – C, D and E

As per the Shared Responsibility Model, the Patching of the underlying hardware and physical security of AWS resources is the responsibility of AWS.

For more information on AWS Shared Responsibility Model, please refer to the below URL-

- https://aws.amazon.com/compliance/shared-responsibility-model/

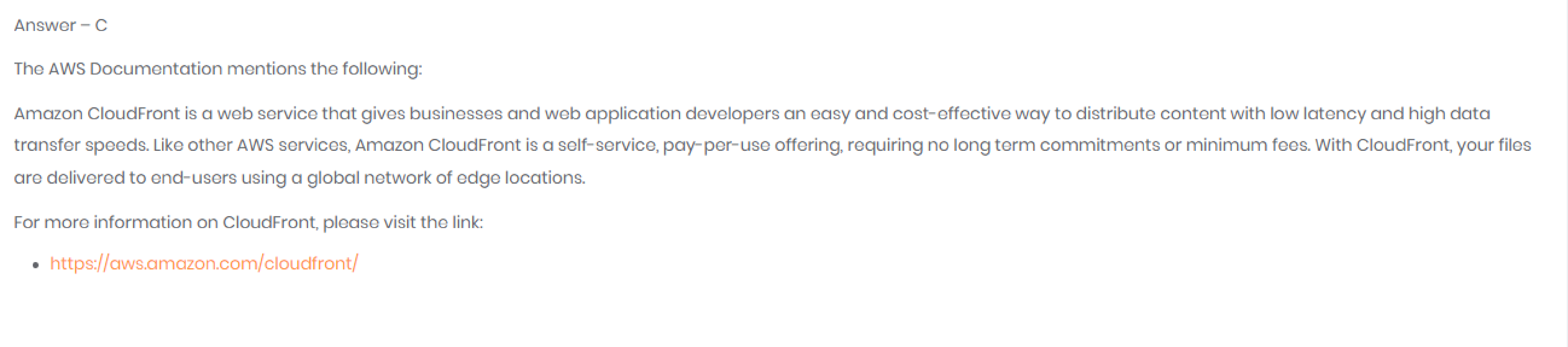
Disk disposal-

Storage Device Decommissioning: When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

For more information on Disk disposal, please refer to the below URL-

- https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

Ques No : 23



Answer – C

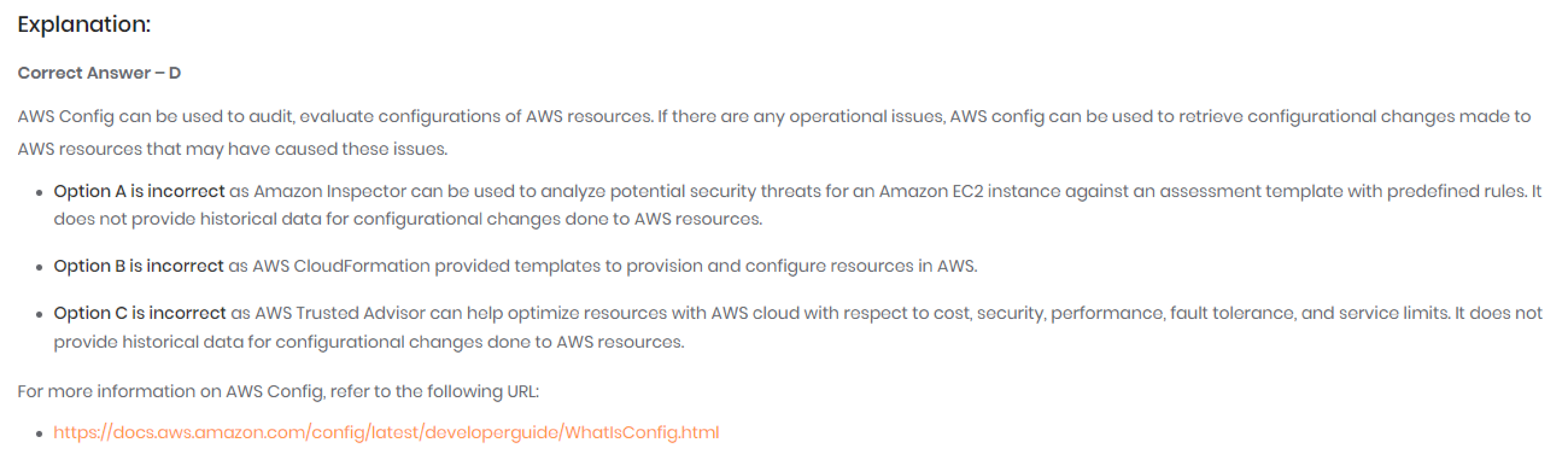
The AWS Documentation mentions the following:

Amazon CloudFront is a web service that gives businesses and web application developers an easy and cost-effective way to distribute content with low latency and high data transfer speeds. Like other AWS services, Amazon CloudFront is a self-service, pay-per-use offering, requiring no long term commitments or minimum fees. With CloudFront, your files are delivered to end-users using a global network of edge locations.

For more information on CloudFront, please visit the link:

- https://aws.amazon.com/cloudfront/

Ques No : 24



Explanation:

Correct Answer – D

AWS Config can be used to audit, evaluate configurations of AWS resources. If there are any operational issues, AWS config can be used to retrieve configurational changes made to AWS resources that may have caused these issues.

- **Option A is incorrect** as Amazon Inspector can be used to analyze potential security threats for an Amazon EC2 instance against an assessment template with predefined rules. It does not provide historical data for configurational changes done to AWS resources.

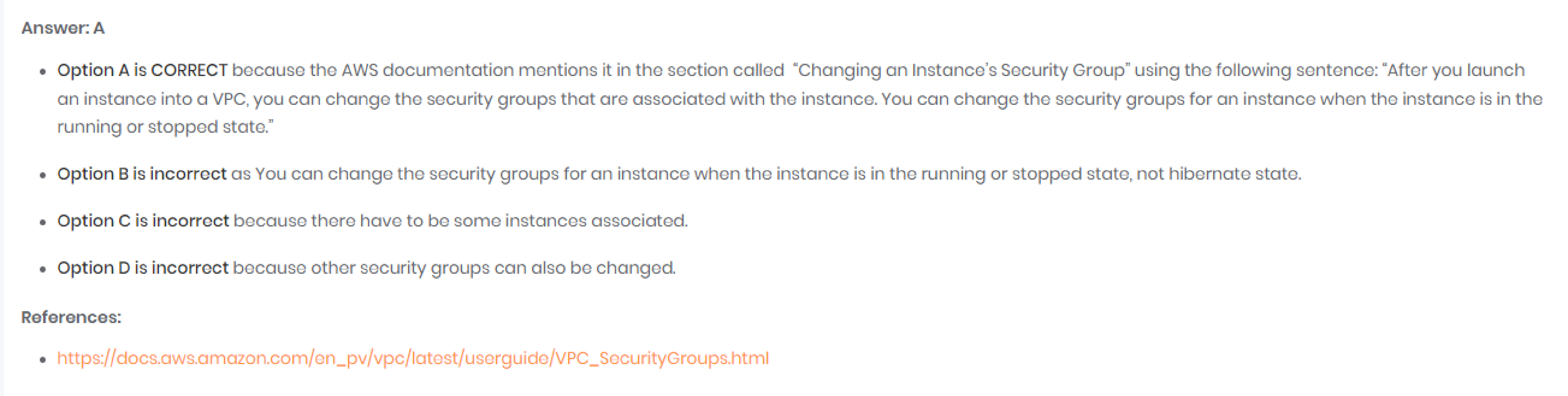
- **Option B is incorrect** as AWS CloudFormation provided templates to provision and configure resources in AWS.

- **Option C is incorrect** as AWS Trusted Advisor can help optimize resources with AWS cloud with respect to cost, security, performance, fault tolerance, and service limits. It does not provide historical data for configurational changes done to AWS resources.

For more information on AWS Config, refer to the following URL:

- https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html

Ques No : 25



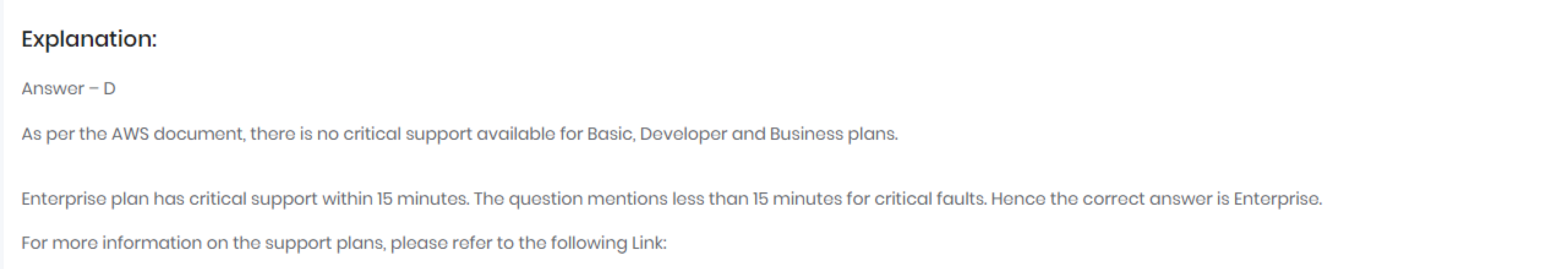
Answer: A

- **Option A is CORRECT** because the AWS documentation mentions it in the section called "Changing an Instance's Security Group" using the following sentence: "After you launch an instance into a VPC, you can change the security groups that are associated with the instance. You can change the security groups for an instance when the instance is in the running or stopped state."
- **Option B is incorrect** as You can change the security groups for an instance when the instance is in the running or stopped state, not hibernate state.
- **Option C is incorrect** because there have to be some instances associated.
- **Option D is incorrect** because other security groups can also be changed.

References:

- https://docs.aws.amazon.com/en_pv/vpc/latest/userguide/VPC_SecurityGroups.html

Ques No : 26



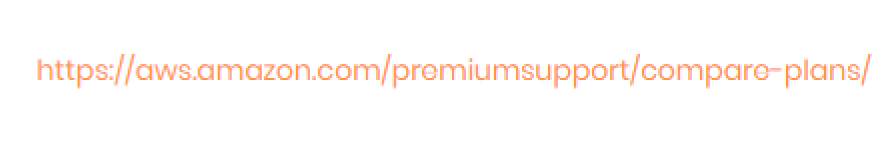
Explanation:

Answer – D

As per the AWS document, there is no critical support available for Basic, Developer and Business plans.

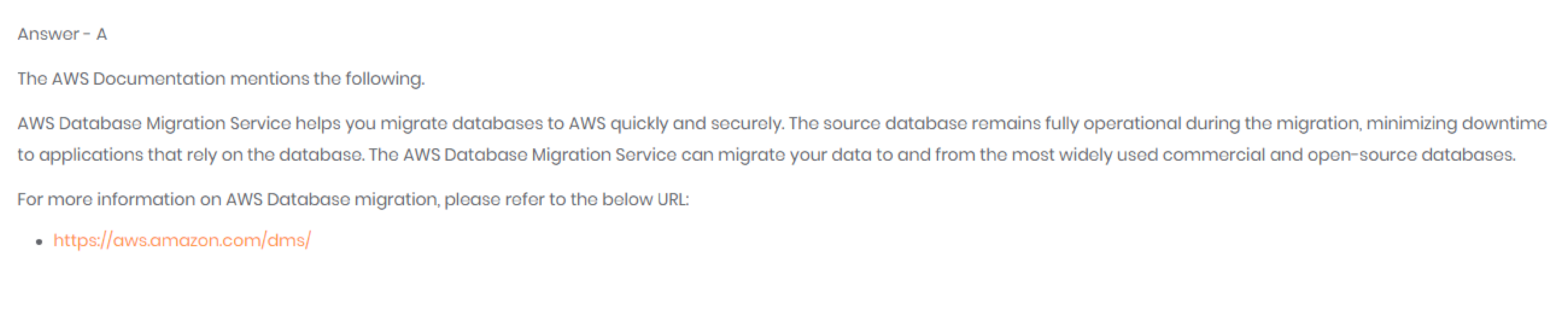
Enterprise plan has critical support within 15 minutes. The question mentions less than 15 minutes for critical faults. Hence the correct answer is Enterprise.

For more information on the support plans, please refer to the following Link:



https://aws.amazon.com/premiumsupport/compare-plans/

Ques No : 27



Answer - A

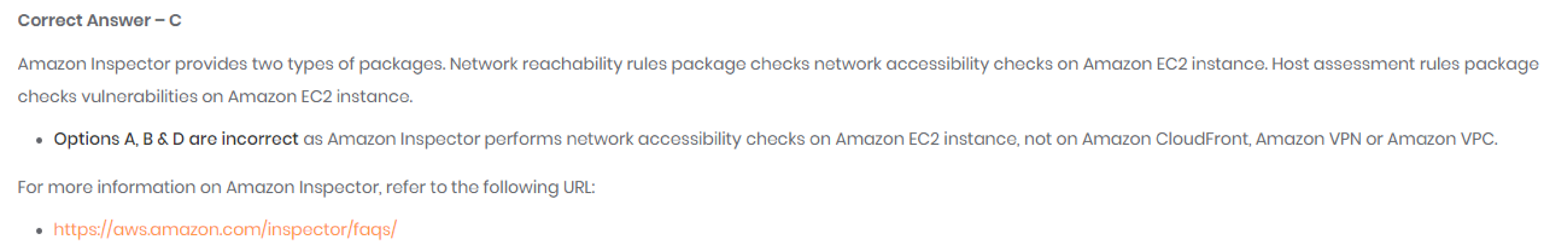
The AWS Documentation mentions the following.

AWS Database Migration Service helps you migrate databases to AWS quickly and securely. The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database. The AWS Database Migration Service can migrate your data to and from the most widely used commercial and open-source databases.

For more information on AWS Database migration, please refer to the below URL:

- https://aws.amazon.com/dms/

Ques No : 28



Correct Answer – C

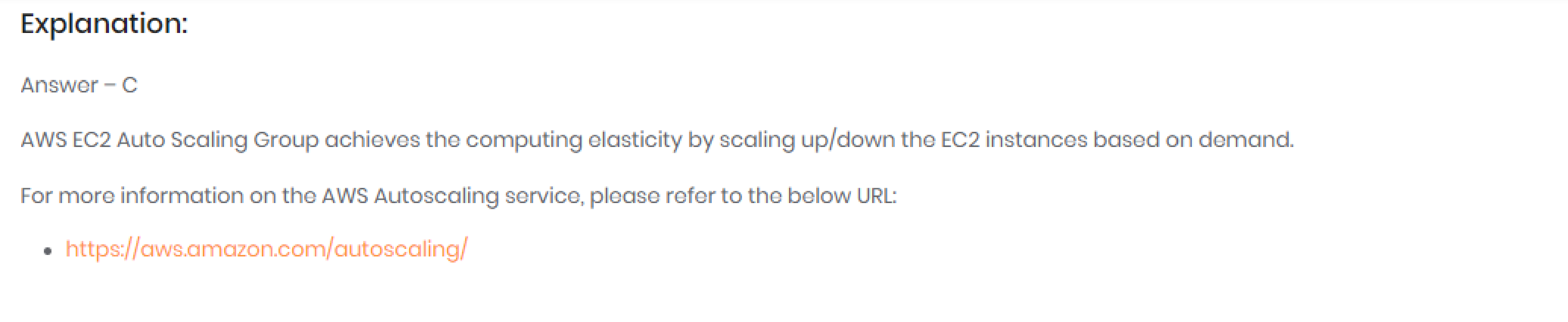
Amazon Inspector provides two types of packages. Network reachability rules package checks network accessibility checks on Amazon EC2 instance. Host assessment rules package checks vulnerabilities on Amazon EC2 instance.

- **Options A, B & D are incorrect** as Amazon Inspector performs network accessibility checks on Amazon EC2 instance, not on Amazon CloudFront, Amazon VPN or Amazon VPC.

For more information on Amazon Inspector, refer to the following URL:

- https://aws.amazon.com/inspector/faqs/

Ques No : 29



Explanation:

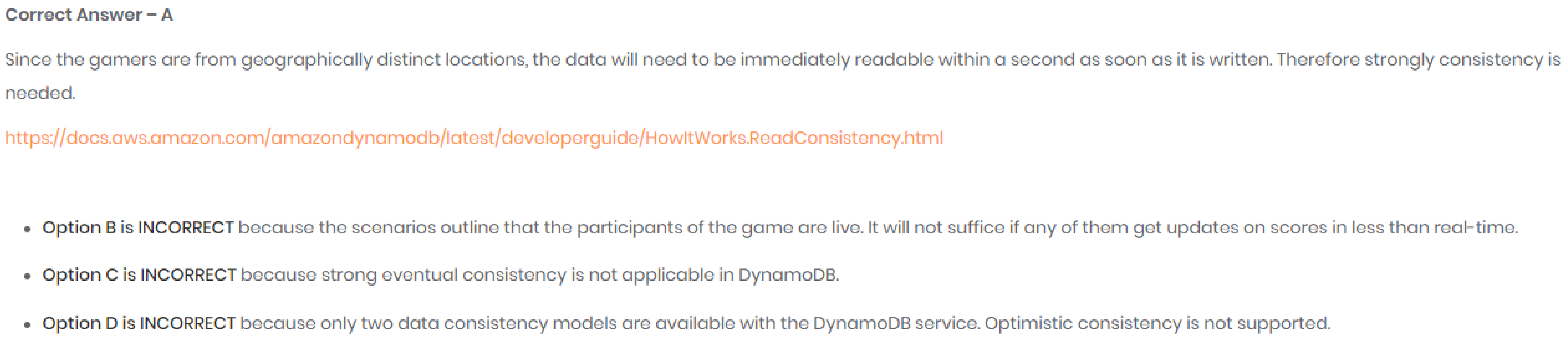
Answer – C

AWS EC2 Auto Scaling Group achieves the computing elasticity by scaling up/down the EC2 instances based on demand.

For more information on the AWS Autoscaling service, please refer to the below URL:

- https://aws.amazon.com/autoscaling/

Ques No : 30



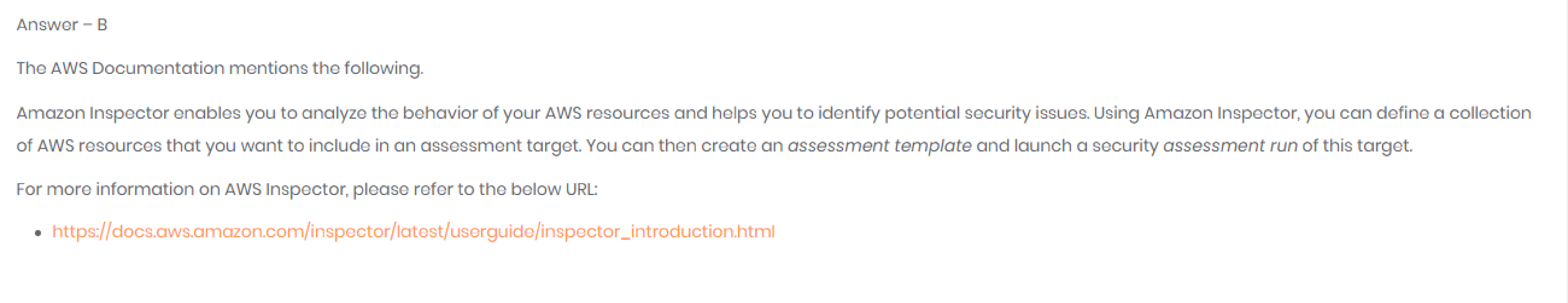
Correct Answer – A

Since the gamers are from geographically distinct locations, the data will need to be immediately readable within a second as soon as it is written. Therefore strongly consistency is needed.

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadConsistency.html

- **Option B is INCORRECT** because the scenarios outline that the participants of the game are live. It will not suffice if any of them get updates on scores in less than real-time.
- **Option C is INCORRECT** because strong eventual consistency is not applicable in DynamoDB.
- **Option D is INCORRECT** because only two data consistency models are available with the DynamoDB service. Optimistic consistency is not supported.

Ques No : 31



Answer – B

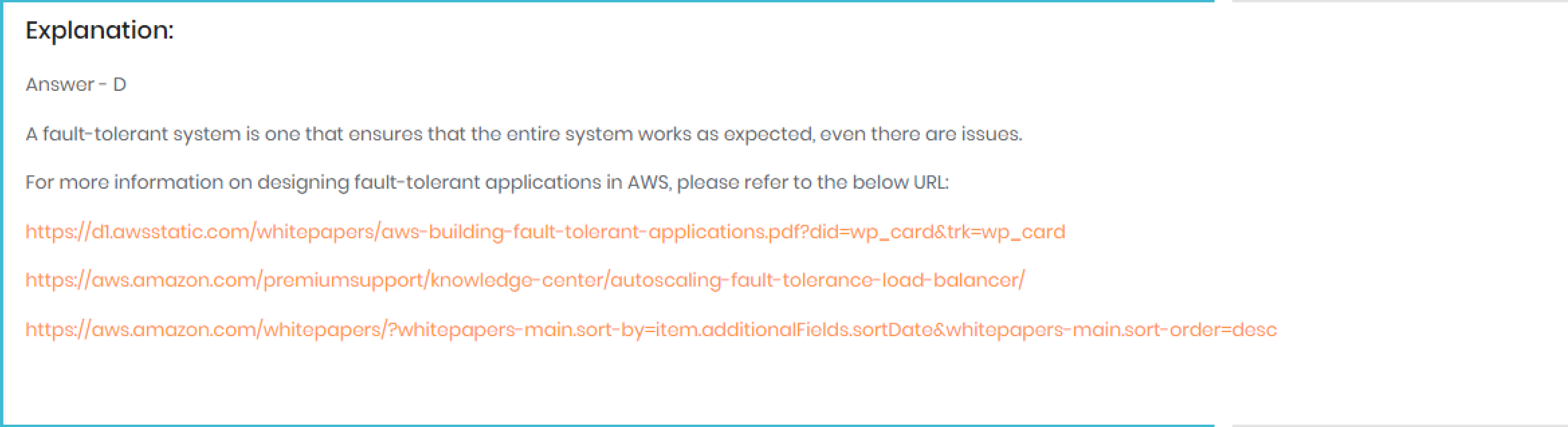
The AWS Documentation mentions the following.

Amazon Inspector enables you to analyze the behavior of your AWS resources and helps you to identify potential security issues. Using Amazon Inspector, you can define a collection of AWS resources that you want to include in an assessment target. You can then create an *assessment template* and launch a security *assessment run* of this target.

For more information on AWS Inspector, please refer to the below URL:

- https://docs.aws.amazon.com/inspector/latest/userguide/inspector_introduction.html

Ques No : 32



Explanation:

Answer - D

A fault-tolerant system is one that ensures that the entire system works as expected, even there are issues.

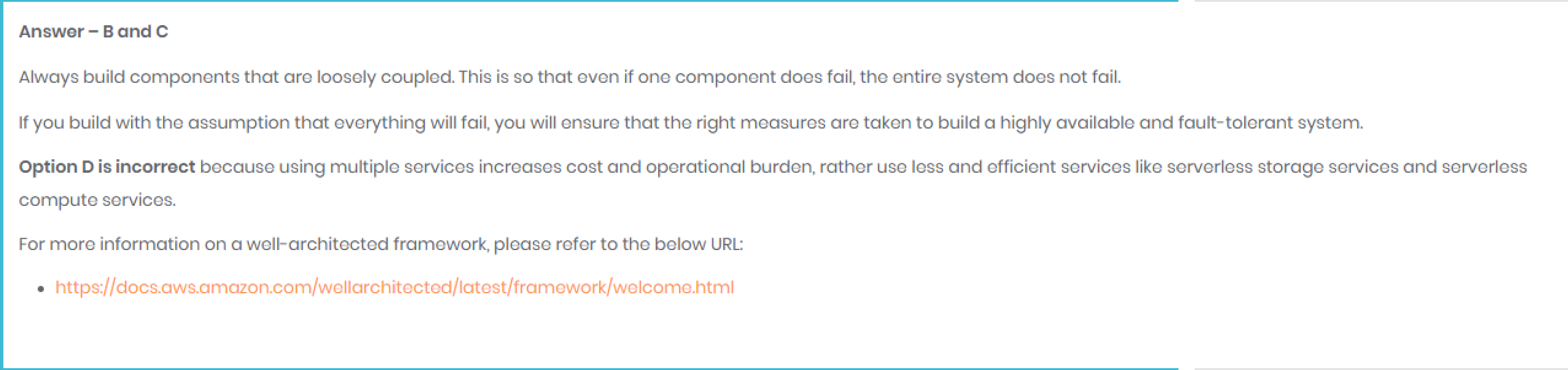
For more information on designing fault-tolerant applications in AWS, please refer to the below URL:

https://d1.awsstatic.com/whitepapers/aws-building-fault-tolerant-applications.pdf?did=wp_card&trk=wp_card

https://aws.amazon.com/premiumsupport/knowledge-center/autoscaling-fault-tolerance-load-balancer/

https://aws.amazon.com/whitepapers/?whitepapers-main.sort-by=item.additionalFields.sortDate&whitepapers-main.sort-order=desc

Ques No : 33



Answer – B and C

Always build components that are loosely coupled. This is so that even if one component does fail, the entire system does not fail.

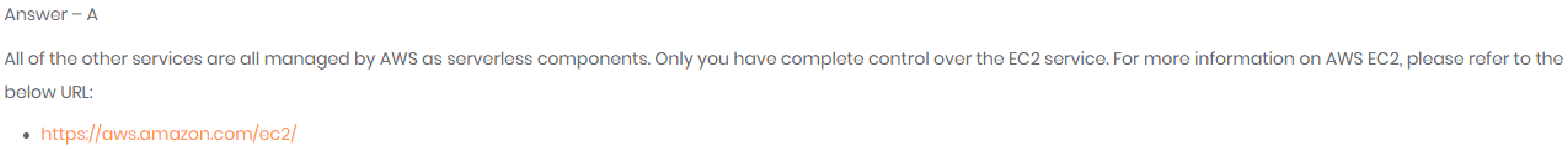
If you build with the assumption that everything will fail, you will ensure that the right measures are taken to build a highly available and fault-tolerant system.

Option D is incorrect because using multiple services increases cost and operational burden, rather use less and efficient services like serverless storage services and serverless compute services.

For more information on a well-architected framework, please refer to the below URL:

- https://docs.aws.amazon.com/wellarchitected/latest/framework/welcome.html

Ques No : 34

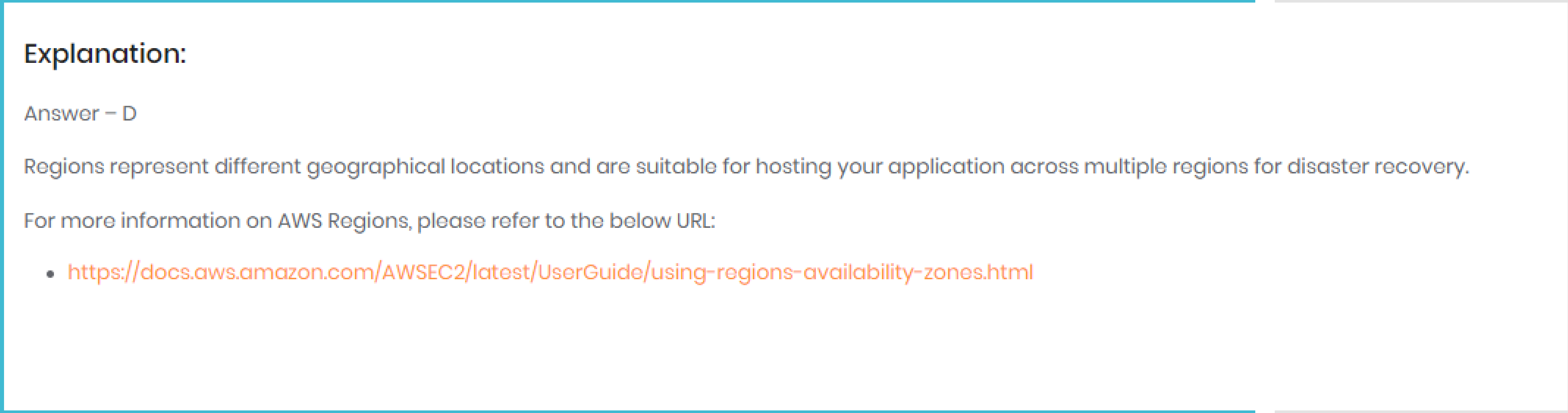


Answer – A

All of the other services are all managed by AWS as serverless components. Only you have complete control over the EC2 service. For more information on AWS EC2, please refer to the below URL:

- https://aws.amazon.com/ec2/

Ques No : 35



Explanation:

Answer – D

Regions represent different geographical locations and are suitable for hosting your application across multiple regions for disaster recovery.

For more information on AWS Regions, please refer to the below URL:

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

Ques No. 36

Answer – C and D

The AWS Documentation mentions the following:

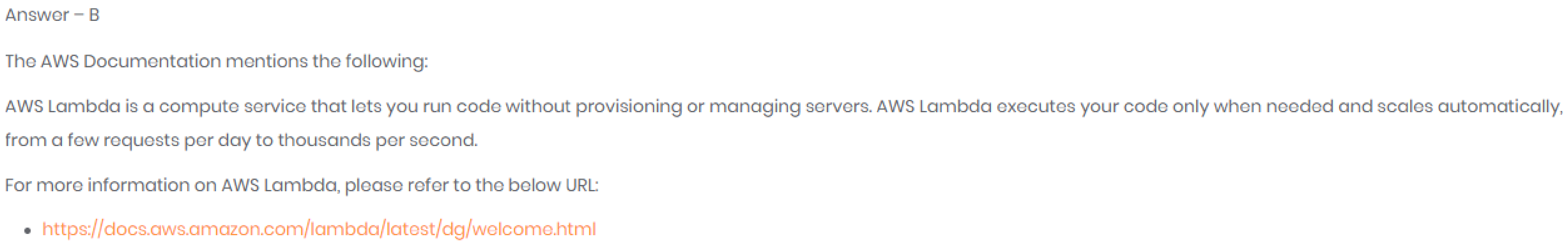
AWS Shield - All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your web site or applications

AWS Shield Advanced - For higher levels of protection against attacks targeting your web applications running on Amazon EC2, Elastic Load Balancing (ELB), CloudFront, and Route 53 resources, you can subscribe to AWS Shield Advanced. AWS Shield Advanced provides expanded DDoS attack protection for these resources.

For more information on AWS Shield, please refer to the below URL:

- https://docs.aws.amazon.com/waf/latest/developerguide/ddos-overview.html

Ques No : 37



Answer – B

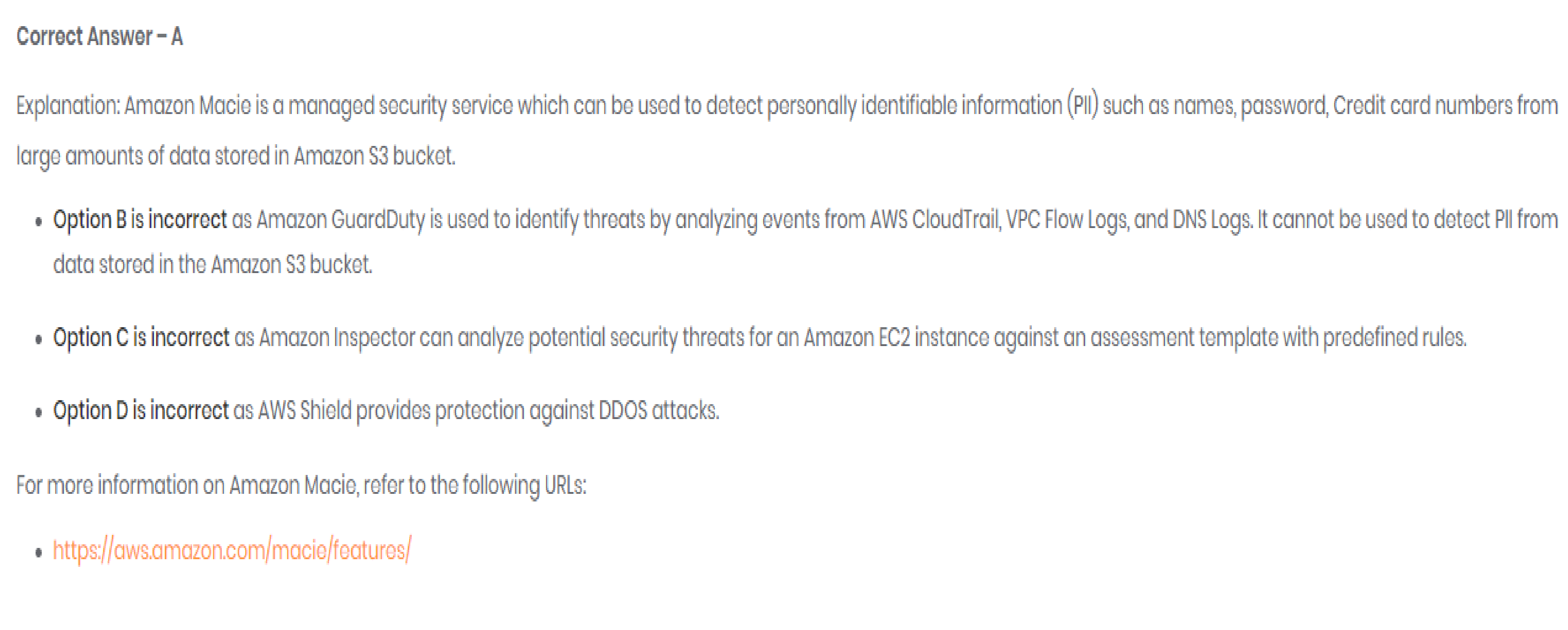
The AWS Documentation mentions the following:

AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second.

For more information on AWS Lambda, please refer to the below URL:

- https://docs.aws.amazon.com/lambda/latest/dg/welcome.html

Ques No : 38



Correct Answer – A

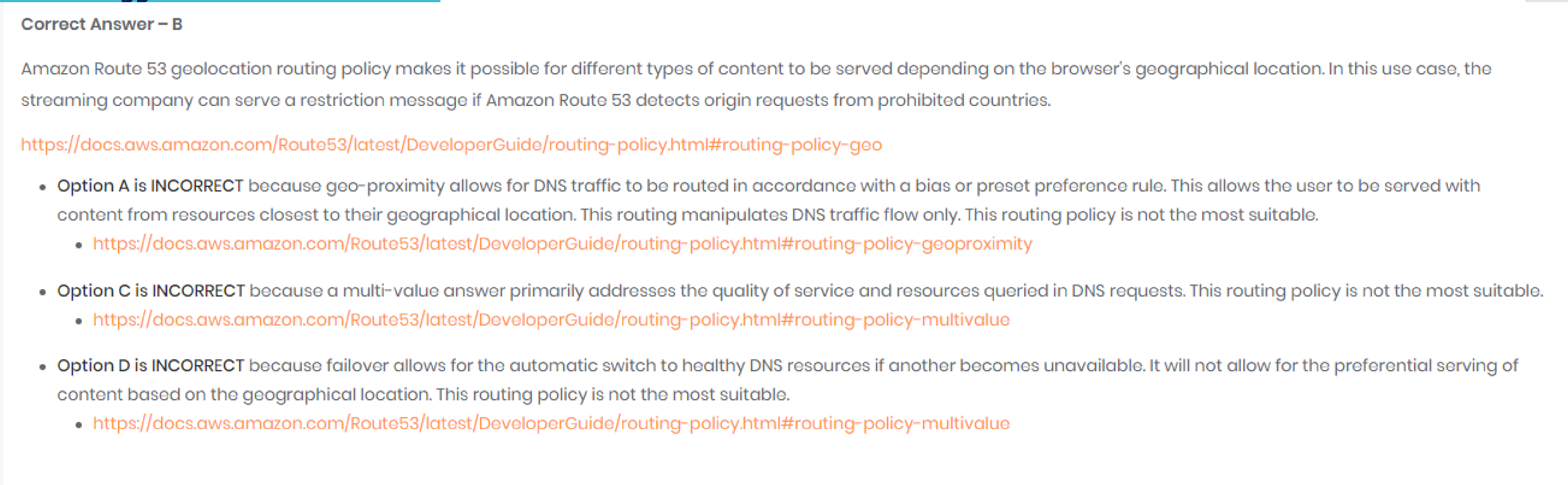
Explanation: Amazon Macie is a managed security service which can be used to detect personally identifiable information (PII) such as names, password, Credit card numbers from large amounts of data stored in Amazon S3 bucket.

- **Option B is incorrect** as Amazon GuardDuty is used to identify threats by analyzing events from AWS CloudTrail, VPC Flow Logs, and DNS Logs. It cannot be used to detect PII from data stored in the Amazon S3 bucket.
- **Option C is incorrect** as Amazon Inspector can analyze potential security threats for an Amazon EC2 instance against an assessment template with predefined rules.
- **Option D is incorrect** as AWS Shield provides protection against DDOS attacks.

For more information on Amazon Macie, refer to the following URLs:

- https://aws.amazon.com/macie/features/

Ques :39



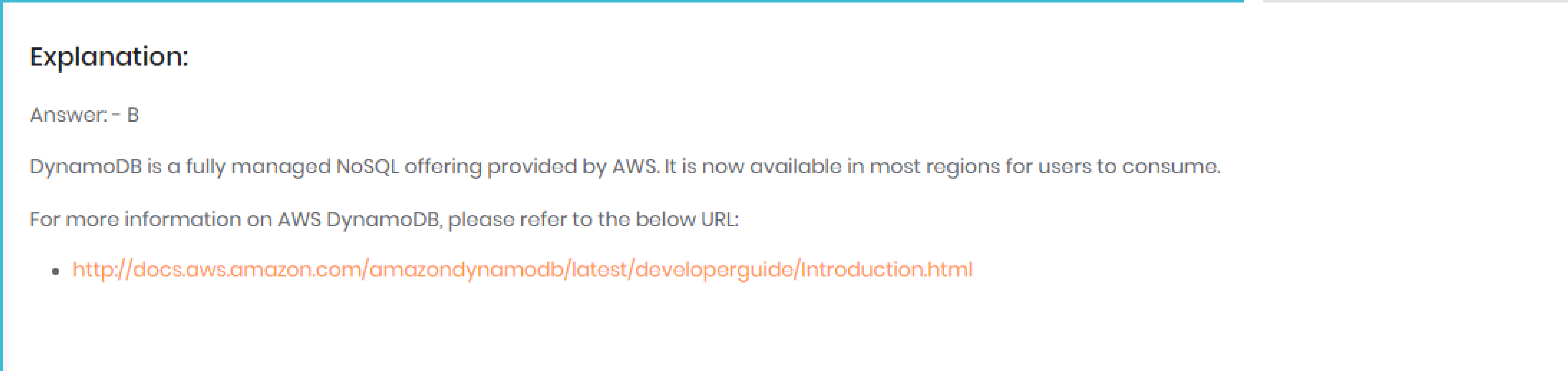
Correct Answer – B

Amazon Route 53 geolocation routing policy makes it possible for different types of content to be served depending on the browser's geographical location. In this use case, the streaming company can serve a restriction message if Amazon Route 53 detects origin requests from prohibited countries.

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-geo

- **Option A is INCORRECT** because geo-proximity allows for DNS traffic to be routed in accordance with a bias or preset preference rule. This allows the user to be served with content from resources closest to their geographical location. This routing manipulates DNS traffic flow only. This routing policy is not the most suitable.
  - https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-geoproximity
- **Option C is INCORRECT** because a multi-value answer primarily addresses the quality of service and resources queried in DNS requests. This routing policy is not the most suitable.
  - https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-multivalue
- **Option D is INCORRECT** because failover allows for the automatic switch to healthy DNS resources if another becomes unavailable. It will not allow for the preferential serving of content based on the geographical location. This routing policy is not the most suitable.
  - https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-multivalue

Ques No : 40



Explanation:

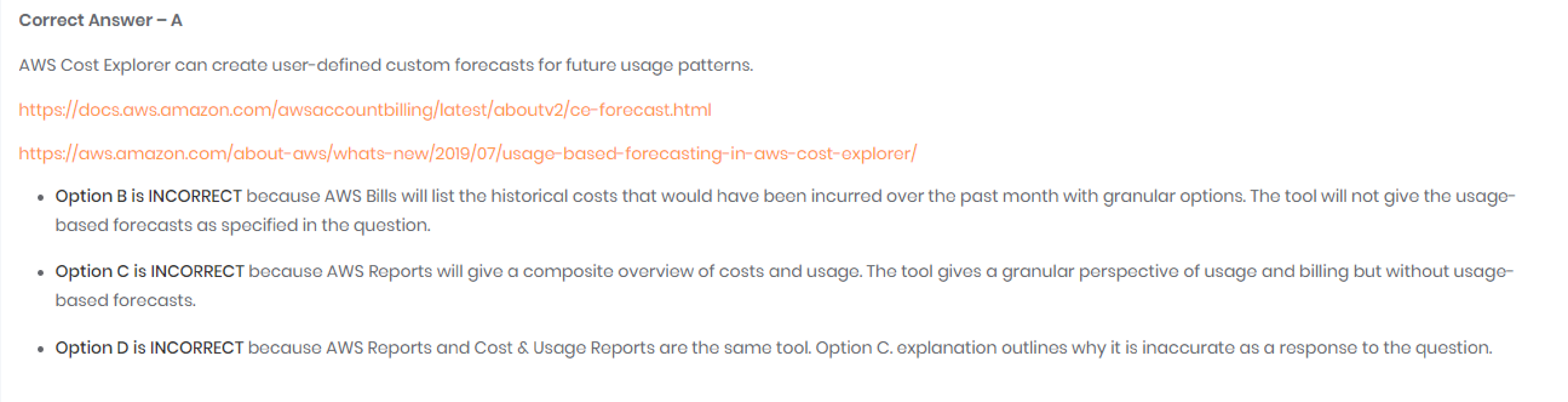
Answer: - B

DynamoDB is a fully managed NoSQL offering provided by AWS. It is now available in most regions for users to consume.

For more information on AWS DynamoDB, please refer to the below URL:

- http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html

Ques No : 41



Correct Answer – A

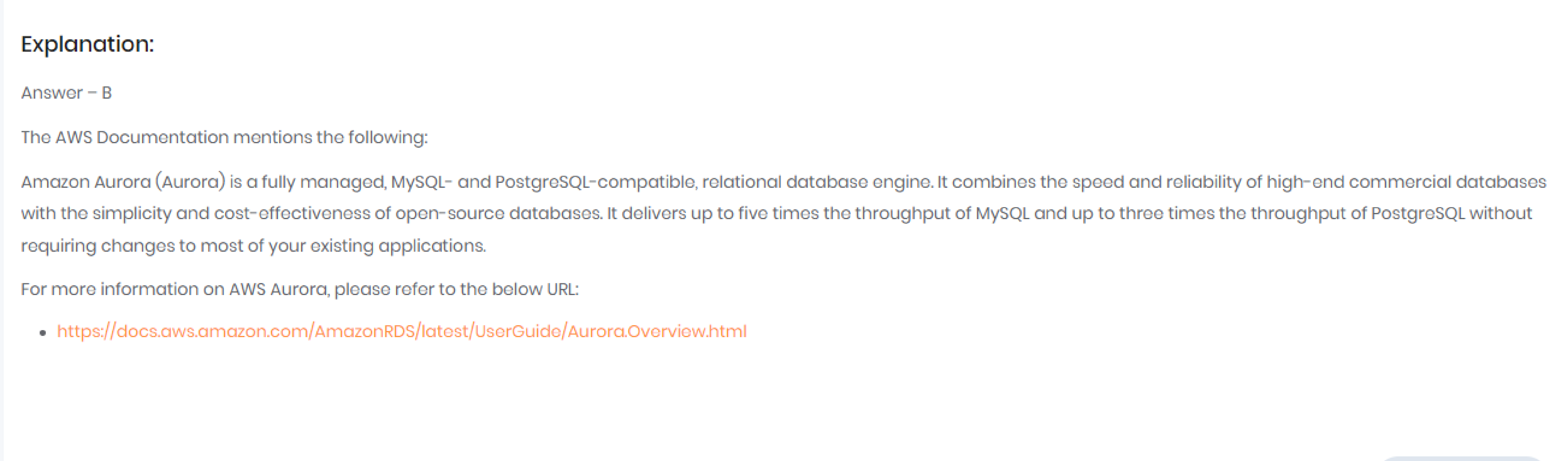
AWS Cost Explorer can create user-defined custom forecasts for future usage patterns.

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ce-forecast.html

https://aws.amazon.com/about-aws/whats-new/2019/07/usage-based-forecasting-in-aws-cost-explorer/

- **Option B is INCORRECT** because AWS Bills will list the historical costs that would have been incurred over the past month with granular options. The tool will not give the usage-based forecasts as specified in the question.
- **Option C is INCORRECT** because AWS Reports will give a composite overview of costs and usage. The tool gives a granular perspective of usage and billing but without usage-based forecasts.
- **Option D is INCORRECT** because AWS Reports and Cost & Usage Reports are the same tool. Option C. explanation outlines why it is inaccurate as a response to the question.

Ques No : 42



Explanation:

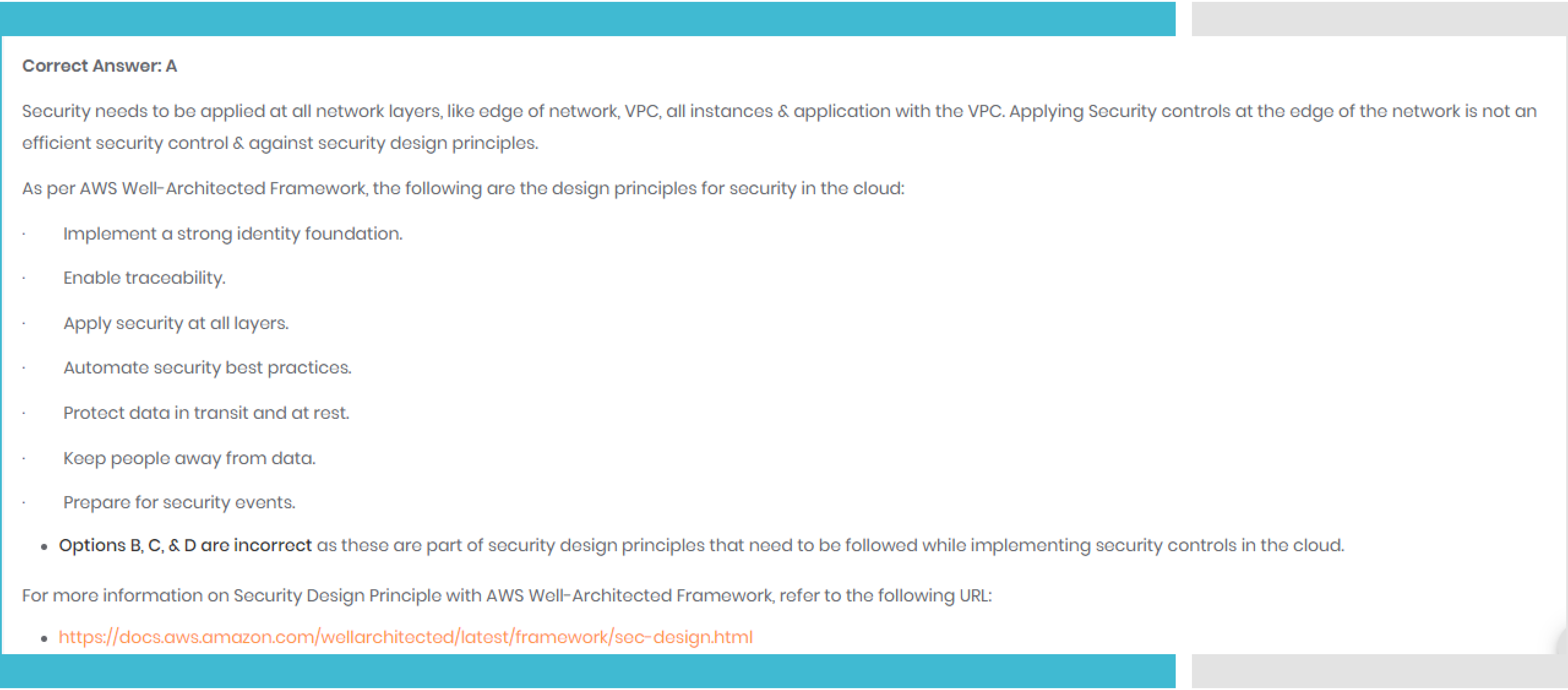
Answer – B

The AWS Documentation mentions the following:

Amazon Aurora (Aurora) is a fully managed, MySQL- and PostgreSQL-compatible, relational database engine. It combines the speed and reliability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. It delivers up to five times the throughput of MySQL and up to three times the throughput of PostgreSQL without requiring changes to most of your existing applications.

For more information on AWS Aurora, please refer to the below URL:

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Aurora.Overview.html



Correct Answer: A

Security needs to be applied at all network layers, like edge of network, VPC, all instances & application with the VPC. Applying Security controls at the edge of the network is not an efficient security control & against security design principles.

As per AWS Well-Architected Framework, the following are the design principles for security in the cloud:

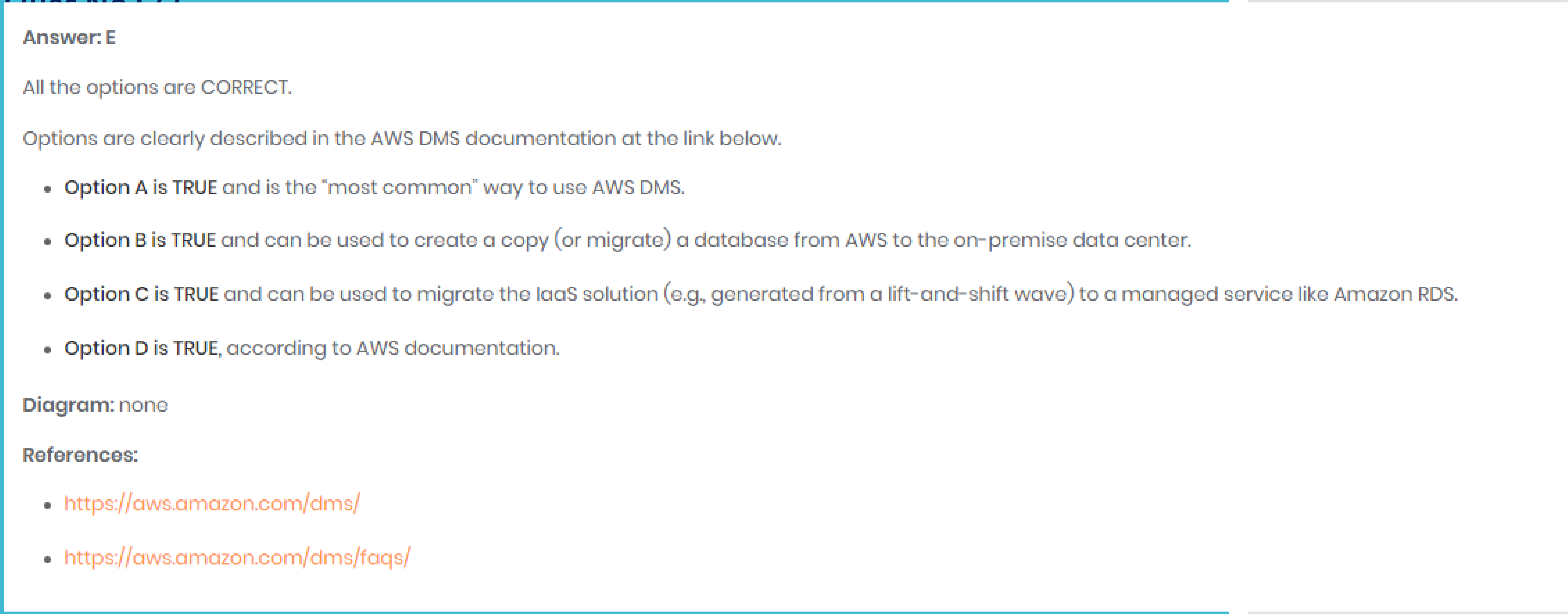
- Implement a strong identity foundation.
- Enable traceability.
- Apply security at all layers.
- Automate security best practices.
- Protect data in transit and at rest.
- Keep people away from data.
- Prepare for security events.

- **Options B, C, & D are incorrect** as these are part of security design principles that need to be followed while implementing security controls in the cloud.

For more information on Security Design Principle with AWS Well-Architected Framework, refer to the following URL:

- https://docs.aws.amazon.com/wellarchitected/latest/framework/sec-design.html

Ques No : 44



Answer: E

All the options are CORRECT.

Options are clearly described in the AWS DMS documentation at the link below.

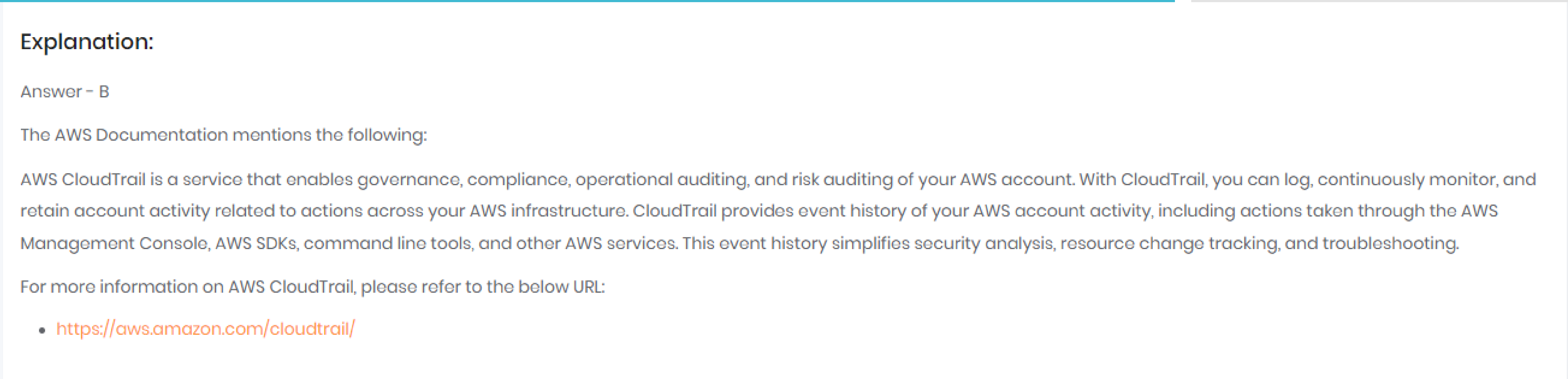
- **Option A is TRUE** and is the "most common" way to use AWS DMS.
- **Option B is TRUE** and can be used to create a copy (or migrate) a database from AWS to the on-premise data center.
- **Option C is TRUE** and can be used to migrate the IaaS solution (e.g., generated from a lift-and-shift wave) to a managed service like Amazon RDS.
- **Option D is TRUE**, according to AWS documentation.

Diagram: none

References:

- https://aws.amazon.com/dms/
- https://aws.amazon.com/dms/faqs/

Ques No : 45



Explanation:

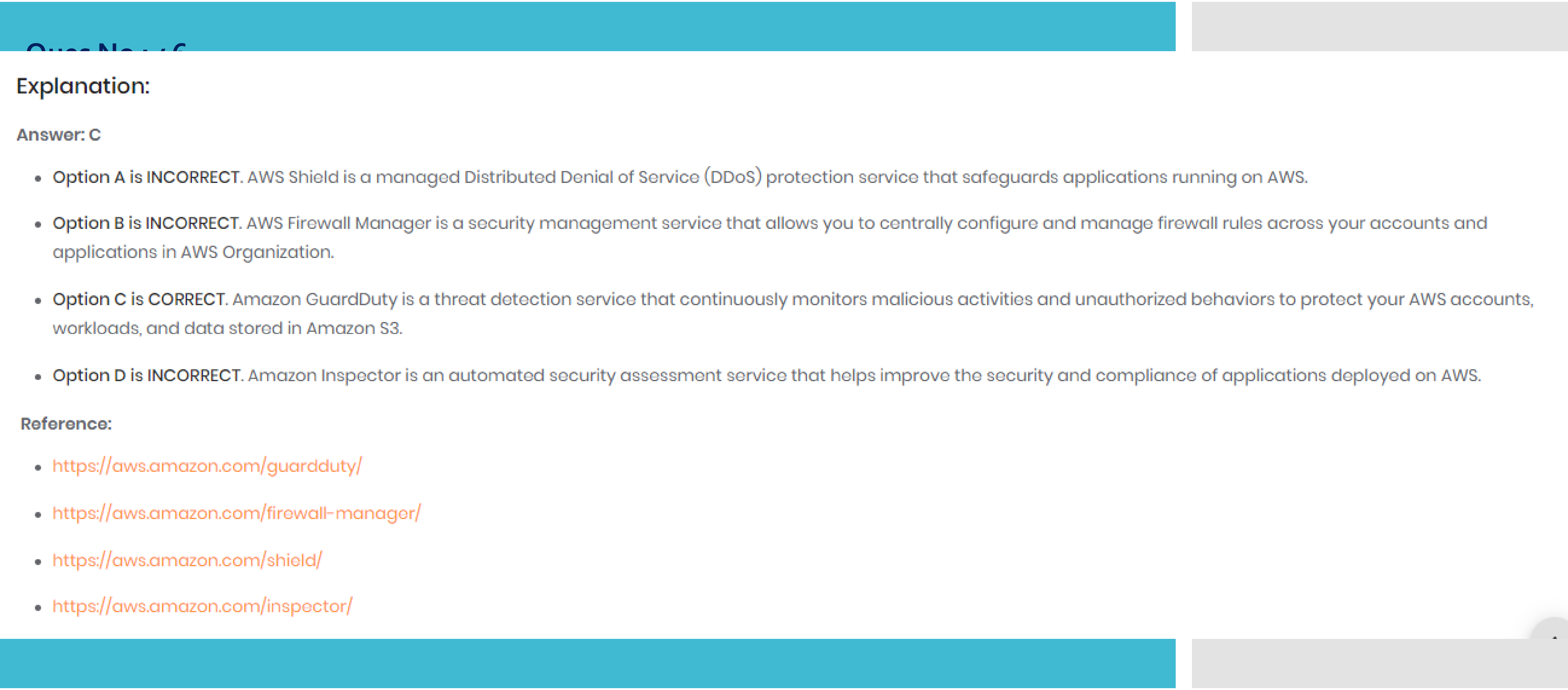
Answer - B

The AWS Documentation mentions the following:

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.

For more information on AWS CloudTrail, please refer to the below URL:

- https://aws.amazon.com/cloudtrail/



Ques No : 6

Explanation:

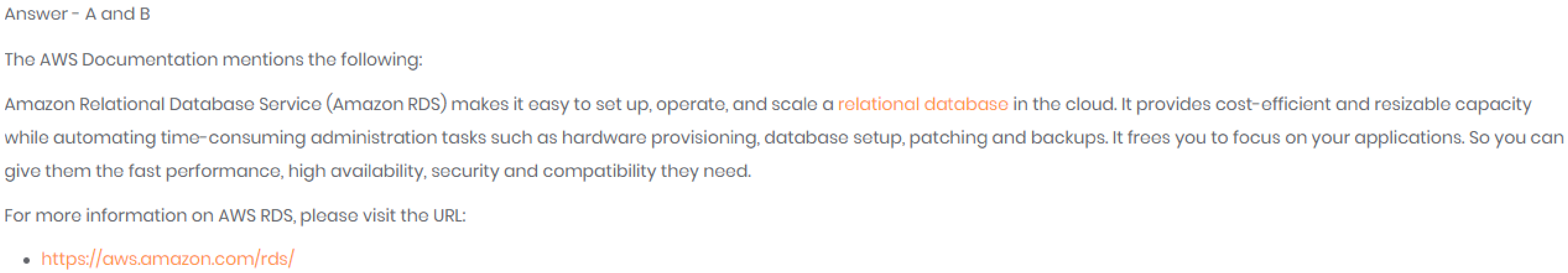
Answer: C

- **Option A is INCORRECT.** AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS.
- **Option B is INCORRECT.** AWS Firewall Manager is a security management service that allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organization.
- **Option C is CORRECT.** Amazon GuardDuty is a threat detection service that continuously monitors malicious activities and unauthorized behaviors to protect your AWS accounts, workloads, and data stored in Amazon S3.
- **Option D is INCORRECT.** Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

Reference:

- https://aws.amazon.com/guardduty/
- https://aws.amazon.com/firewall-manager/
- https://aws.amazon.com/shield/
- https://aws.amazon.com/inspector/

Ques No : 47



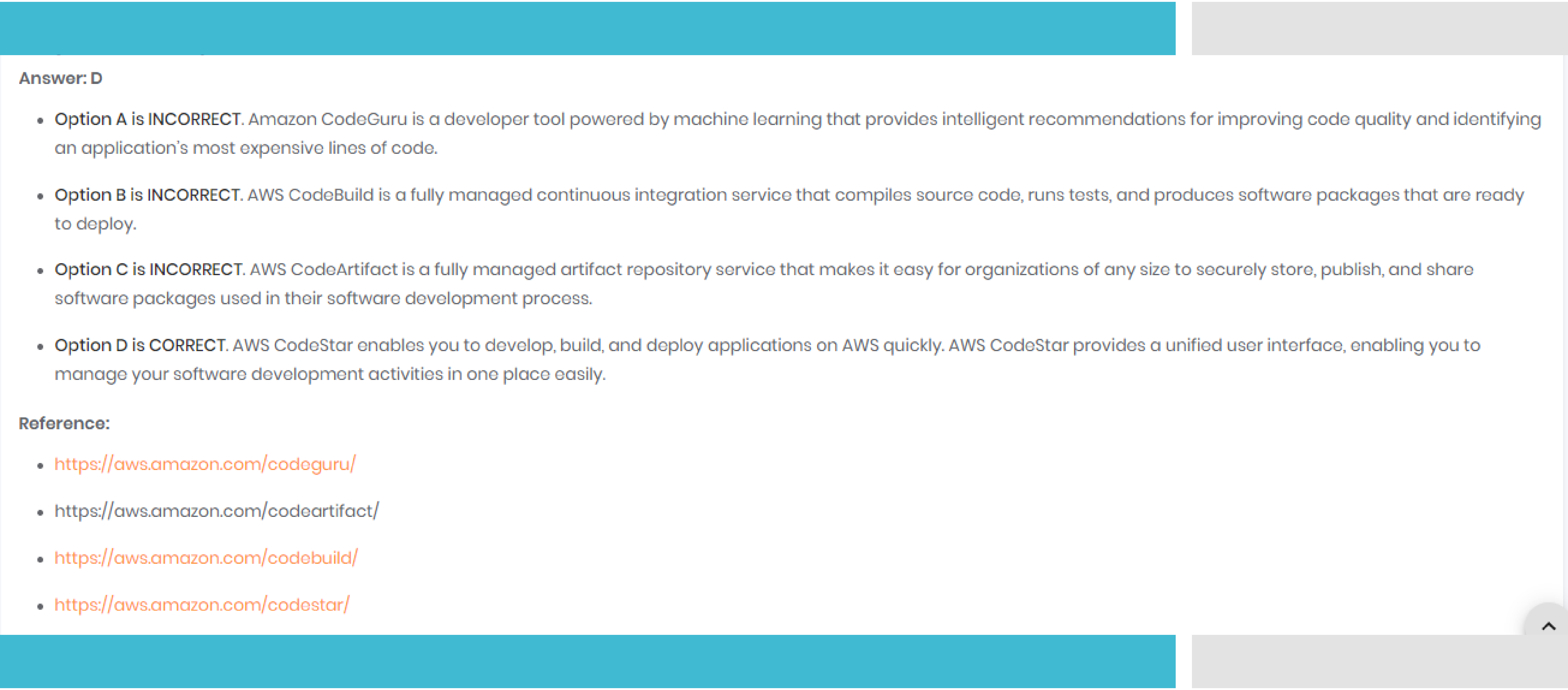
Answer - A and B

The AWS Documentation mentions the following:

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups. It frees you to focus on your applications. So you can give them the fast performance, high availability, security and compatibility they need.

For more information on AWS RDS, please visit the URL:

- https://aws.amazon.com/rds/



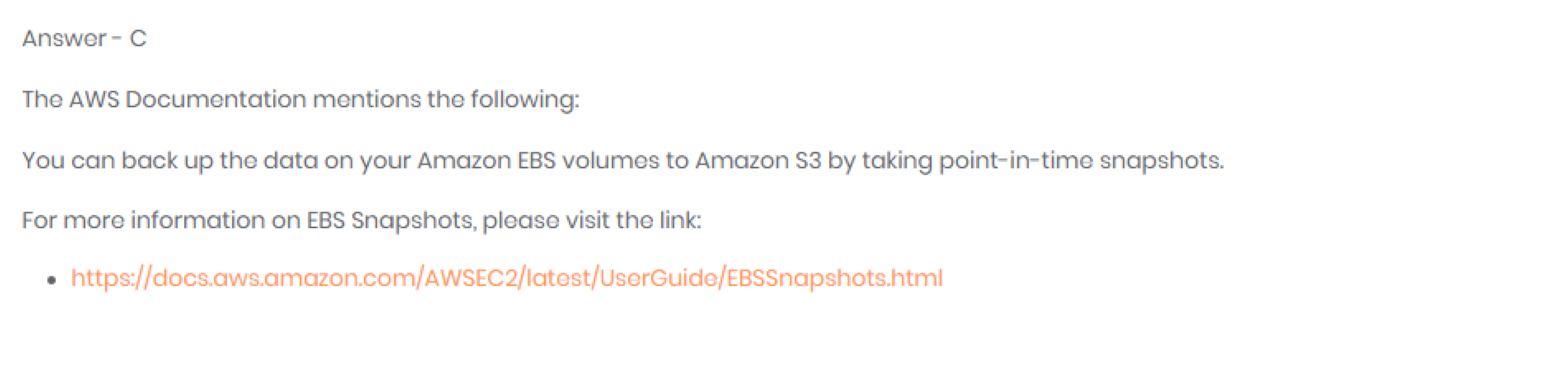
Answer: D

- **Option A is INCORRECT.** Amazon CodeGuru is a developer tool powered by machine learning that provides intelligent recommendations for improving code quality and identifying an application's most expensive lines of code.
- **Option B is INCORRECT.** AWS CodeBuild is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy.
- **Option C is INCORRECT.** AWS CodeArtifact is a fully managed artifact repository service that makes it easy for organizations of any size to securely store, publish, and share software packages used in their software development process.
- **Option D is CORRECT.** AWS CodeStar enables you to develop, build, and deploy applications on AWS quickly. AWS CodeStar provides a unified user interface, enabling you to manage your software development activities in one place easily.

Reference:

- https://aws.amazon.com/codeguru/
- https://aws.amazon.com/codeartifact/
- https://aws.amazon.com/codebuild/
- https://aws.amazon.com/codestar/

Ques No : 49



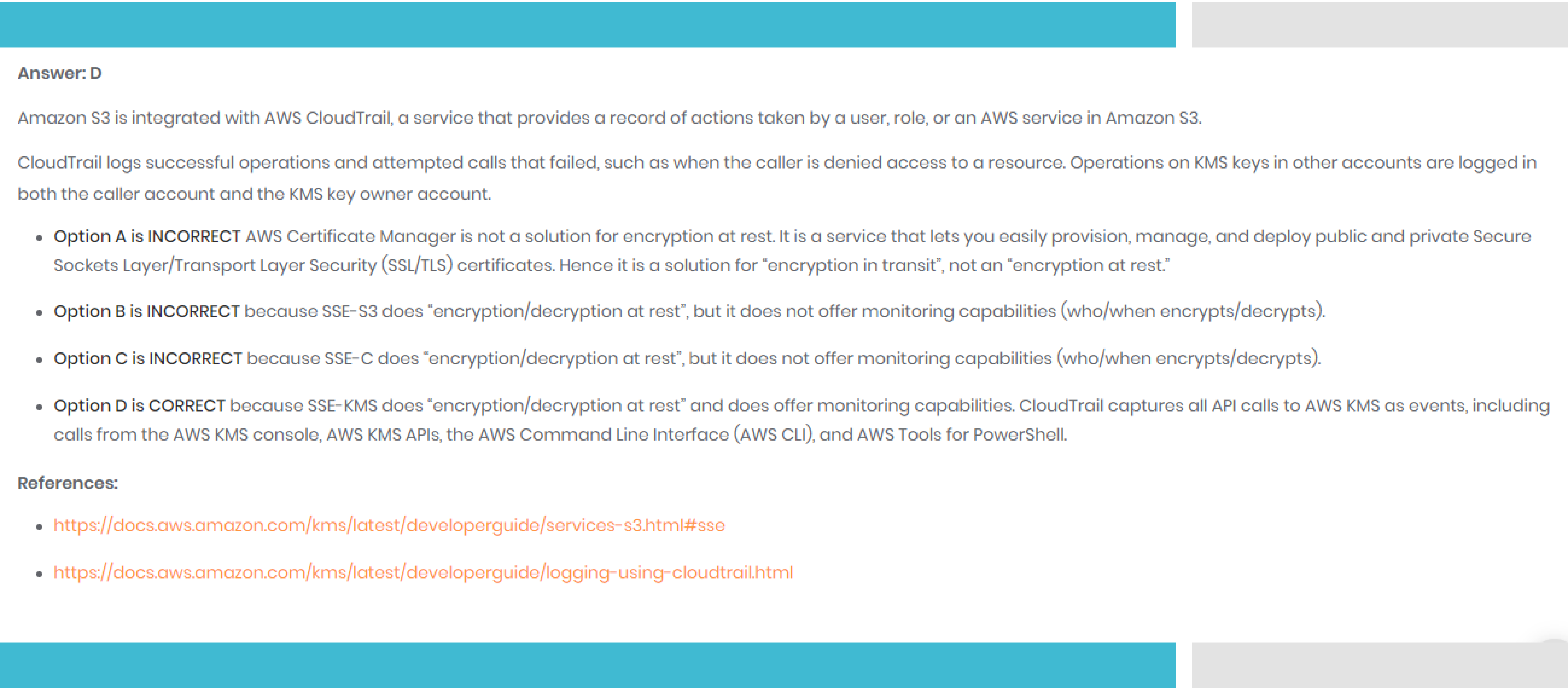
Answer - C

The AWS Documentation mentions the following:

You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots.

For more information on EBS Snapshots, please visit the link:

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html



Answer: D

Amazon S3 is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Amazon S3.

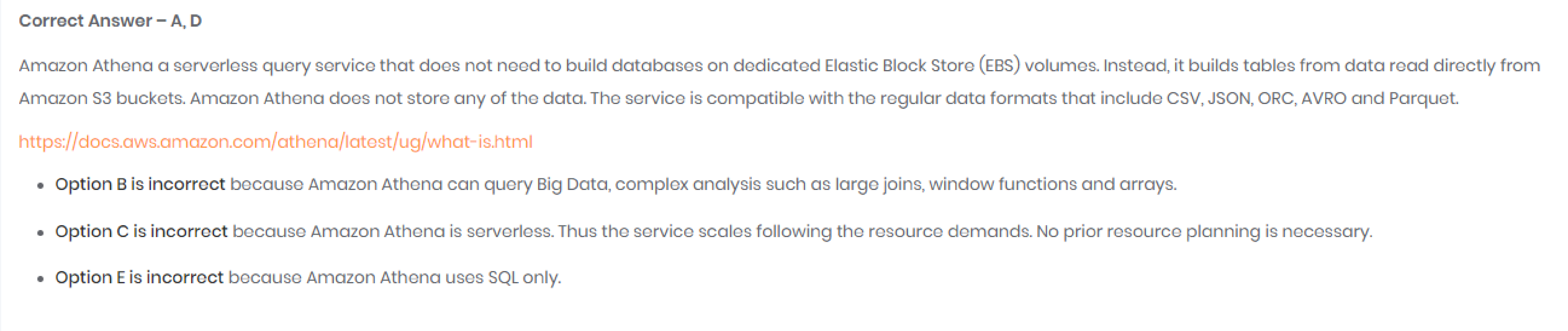
CloudTrail logs successful operations and attempted calls that failed, such as when the caller is denied access to a resource. Operations on KMS keys in other accounts are logged in both the caller account and the KMS key owner account.

- **Option A is INCORRECT** AWS Certificate Manager is not a solution for encryption at rest. It is a service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates. Hence it is a solution for "encryption in transit", not an "encryption at rest."
- **Option B is INCORRECT** because SSE-S3 does "encryption/decryption at rest", but it does not offer monitoring capabilities (who/when encrypts/decrypts).
- **Option C is INCORRECT** because SSE-C does "encryption/decryption at rest", but it does not offer monitoring capabilities (who/when encrypts/decrypts).
- **Option D is CORRECT** because SSE-KMS does "encryption/decryption at rest" and does offer monitoring capabilities. CloudTrail captures all API calls to AWS KMS as events, including calls from the AWS KMS console, AWS KMS APIs, the AWS Command Line Interface (AWS CLI), and AWS Tools for PowerShell.

References:

- https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html#sse
- https://docs.aws.amazon.com/kms/latest/developerguide/logging-using-cloudtrail.html

Ques No : 51



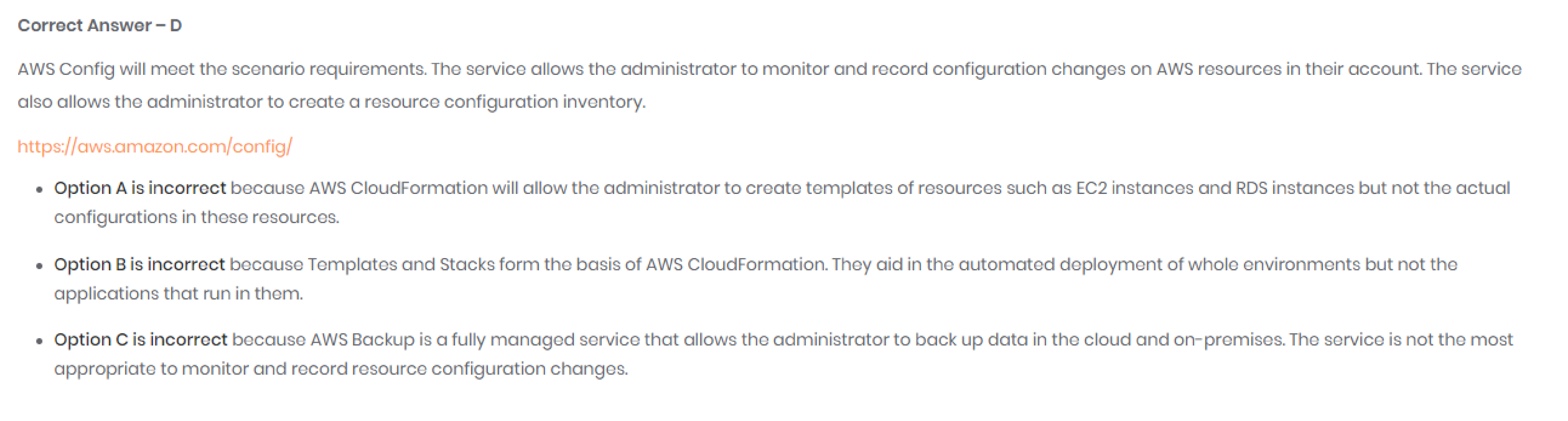
Correct Answer – A, D

Amazon Athena a serverless query service that does not need to build databases on dedicated Elastic Block Store (EBS) volumes. Instead, it builds tables from data read directly from Amazon S3 buckets. Amazon Athena does not store any of the data. The service is compatible with the regular data formats that include CSV, JSON, ORC, AVRO and Parquet.

https://docs.aws.amazon.com/athena/latest/ug/what-is.html

- **Option B is incorrect** because Amazon Athena can query Big Data, complex analysis such as large joins, window functions and arrays.
- **Option C is incorrect** because Amazon Athena is serverless. Thus the service scales following the resource demands. No prior resource planning is necessary.
- **Option E is incorrect** because Amazon Athena uses SQL only.

Ques No : 52



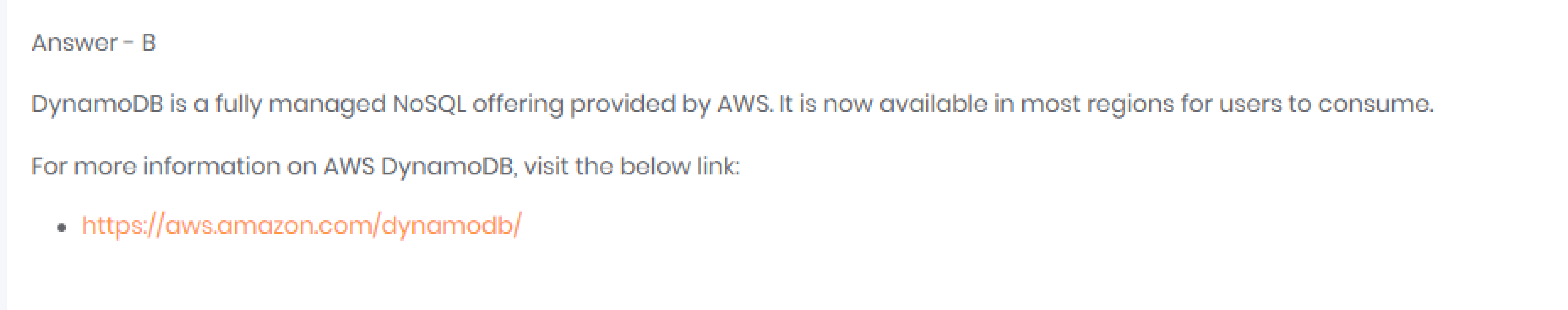
Correct Answer – D

AWS Config will meet the scenario requirements. The service allows the administrator to monitor and record configuration changes on AWS resources in their account. The service also allows the administrator to create a resource configuration inventory.

https://aws.amazon.com/config/

- **Option A is incorrect** because AWS CloudFormation will allow the administrator to create templates of resources such as EC2 instances and RDS instances but not the actual configurations in these resources.
- **Option B is incorrect** because Templates and Stacks form the basis of AWS CloudFormation. They aid in the automated deployment of whole environments but not the applications that run in them.
- **Option C is incorrect** because AWS Backup is a fully managed service that allows the administrator to back up data in the cloud and on-premises. The service is not the most appropriate to monitor and record resource configuration changes.

Ques No : 53



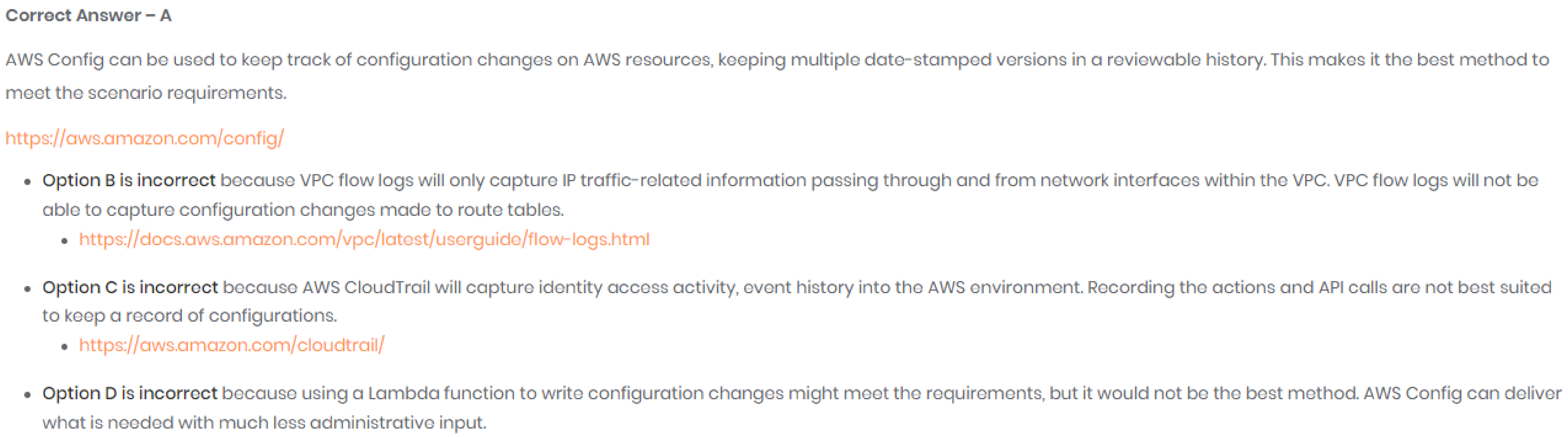
Answer - B

DynamoDB is a fully managed NoSQL offering provided by AWS. It is now available in most regions for users to consume.

For more information on AWS DynamoDB, visit the below link:

- https://aws.amazon.com/dynamodb/

Ques No : 54



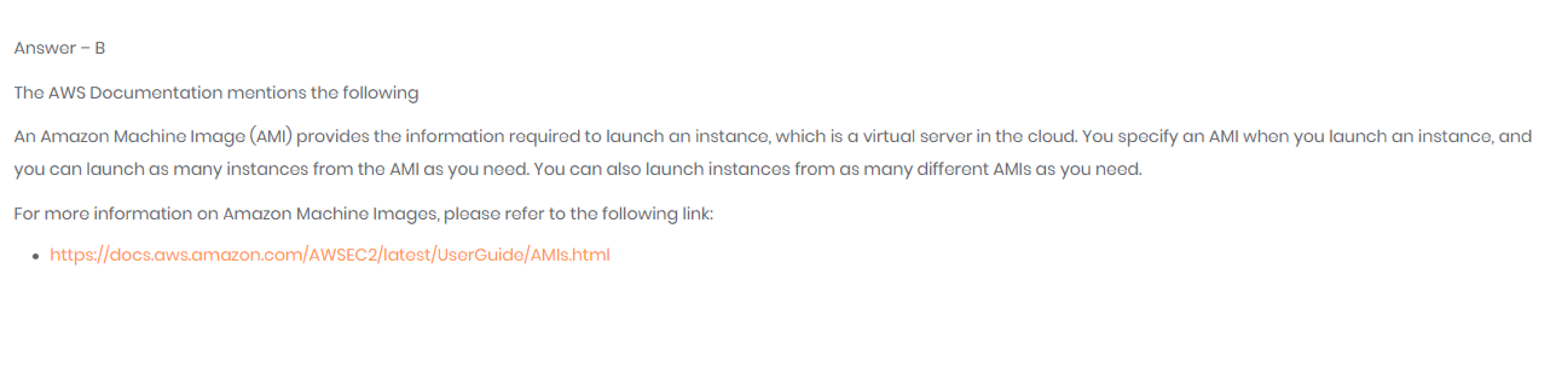
Correct Answer – A

AWS Config can be used to keep track of configuration changes on AWS resources, keeping multiple date-stamped versions in a reviewable history. This makes it the best method to meet the scenario requirements.

https://aws.amazon.com/config/

- **Option B is incorrect** because VPC flow logs will only capture IP traffic-related information passing through and from network interfaces within the VPC. VPC flow logs will not be able to capture configuration changes made to route tables.
  - https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html
- **Option C is incorrect** because AWS CloudTrail will capture identity access activity, event history into the AWS environment. Recording the actions and API calls are not best suited to keep a record of configurations.
  - https://aws.amazon.com/cloudtrail/
- **Option D is incorrect** because using a Lambda function to write configuration changes might meet the requirements, but it would not be the best method. AWS Config can deliver what is needed with much less administrative input.

Ques No : 55



Answer – B

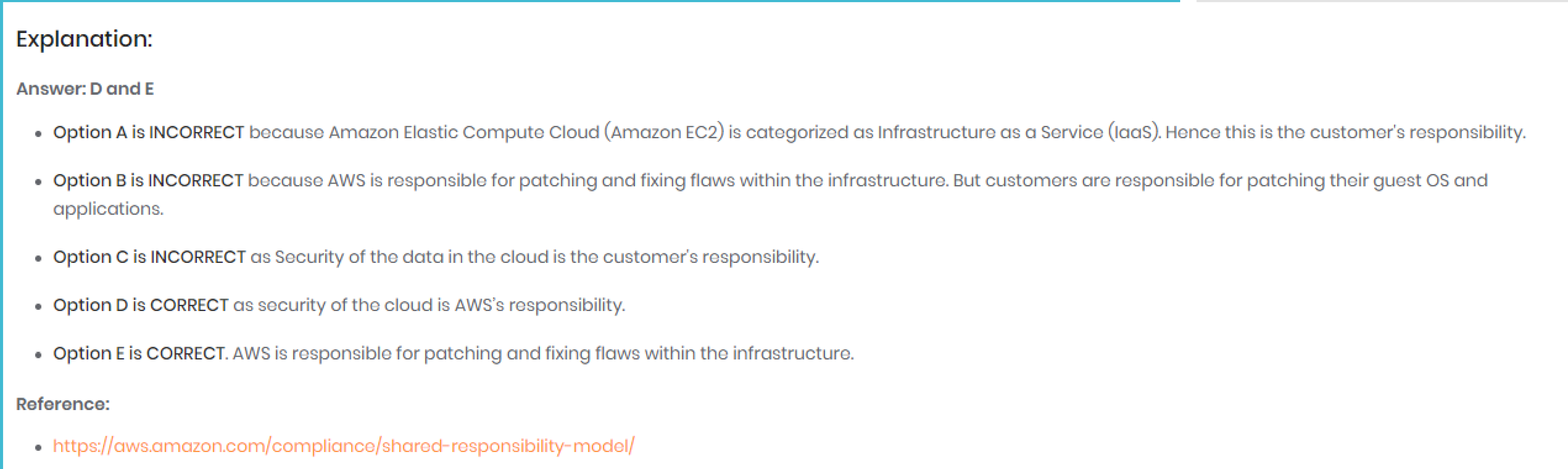
The AWS Documentation mentions the following

An Amazon Machine Image (AMI) provides the information required to launch an instance, which is a virtual server in the cloud. You specify an AMI when you launch an instance, and you can launch as many instances from the AMI as you need. You can also launch instances from as many different AMIs as you need.

For more information on Amazon Machine Images, please refer to the following link:

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html

Ques No : 056



Explanation:

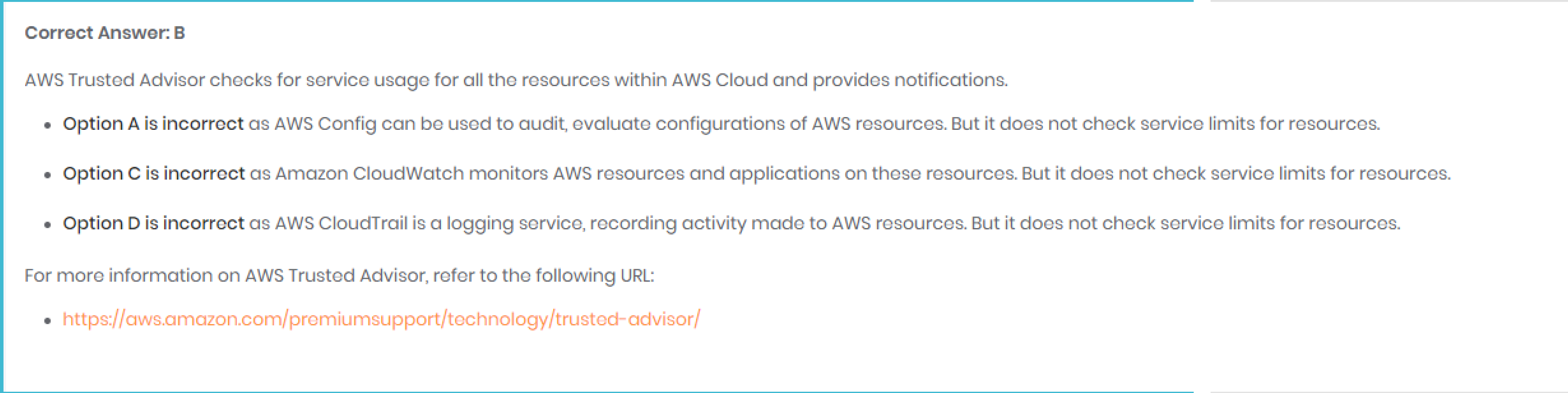
Answer: D and E

- **Option A is INCORRECT** because Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS). Hence this is the customer's responsibility.
- **Option B is INCORRECT** because AWS is responsible for patching and fixing flaws within the infrastructure. But customers are responsible for patching their guest OS and applications.
- **Option C is INCORRECT** as Security of the data in the cloud is the customer's responsibility.
- **Option D is CORRECT** as security of the cloud is AWS's responsibility.
- **Option E is CORRECT**. AWS is responsible for patching and fixing flaws within the infrastructure.

Reference:

- https://aws.amazon.com/compliance/shared-responsibility-model/

Ques No : 57



Correct Answer: B

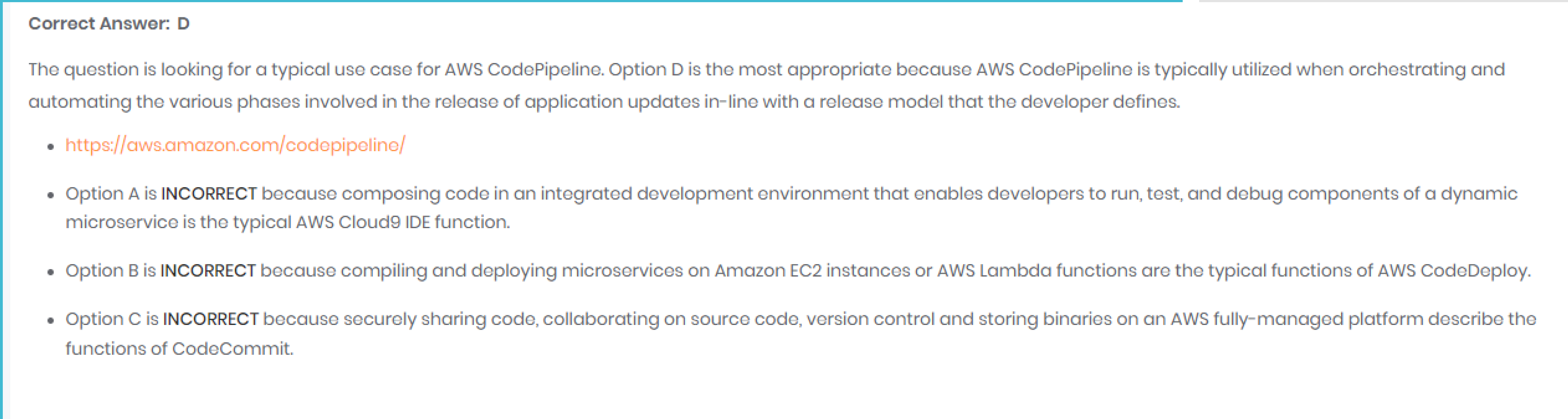
AWS Trusted Advisor checks for service usage for all the resources within AWS Cloud and provides notifications.

- **Option A is incorrect** as AWS Config can be used to audit, evaluate configurations of AWS resources. But it does not check service limits for resources.
- **Option C is incorrect** as Amazon CloudWatch monitors AWS resources and applications on these resources. But it does not check service limits for resources.
- **Option D is incorrect** as AWS CloudTrail is a logging service, recording activity made to AWS resources. But it does not check service limits for resources.

For more information on AWS Trusted Advisor, refer to the following URL:

- https://aws.amazon.com/premiumsupport/technology/trusted-advisor/

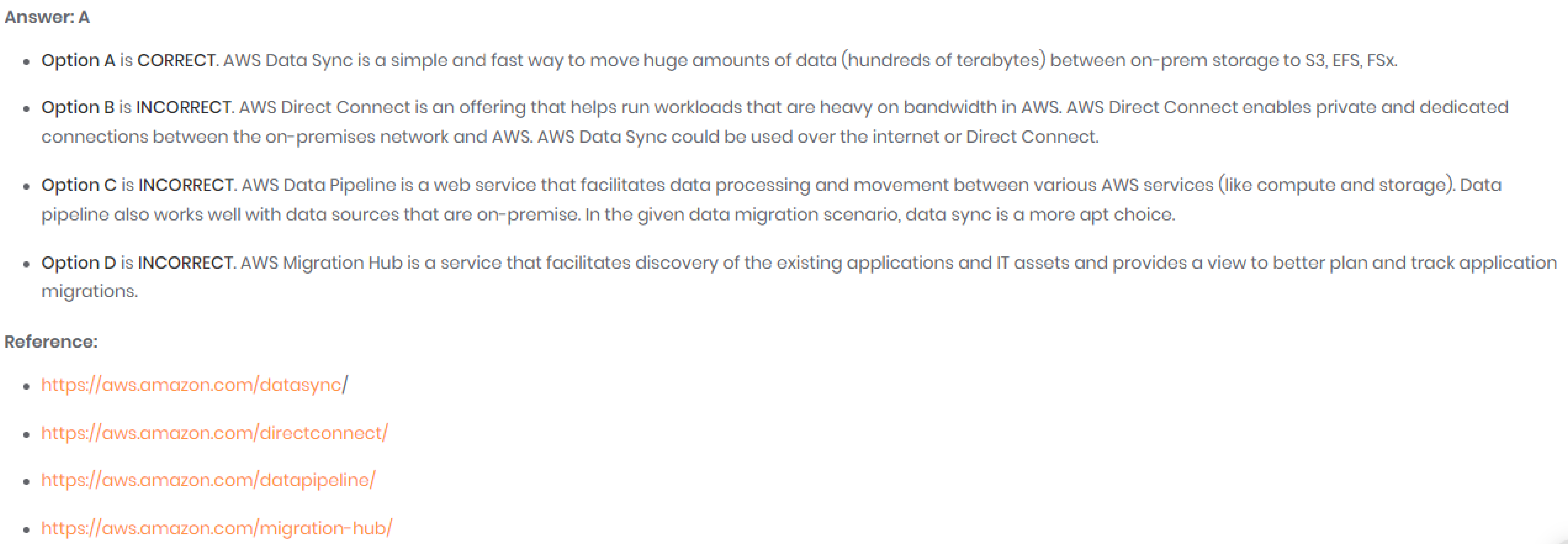
Ques No : 58



Correct Answer: D

The question is looking for a typical use case for AWS CodePipeline. Option D is the most appropriate because AWS CodePipeline is typically utilized when orchestrating and automating the various phases involved in the release of application updates in-line with a release model that the developer defines.

- https://aws.amazon.com/codepipeline/
- Option A is INCORRECT because composing code in an integrated development environment that enables developers to run, test, and debug components of a dynamic microservice is the typical AWS Cloud9 IDE function.
- Option B is INCORRECT because compiling and deploying microservices on Amazon EC2 instances or AWS Lambda functions are the typical functions of AWS CodeDeploy.
- Option C is INCORRECT because securely sharing code, collaborating on source code, version control and storing binaries on an AWS fully-managed platform describe the functions of CodeCommit.

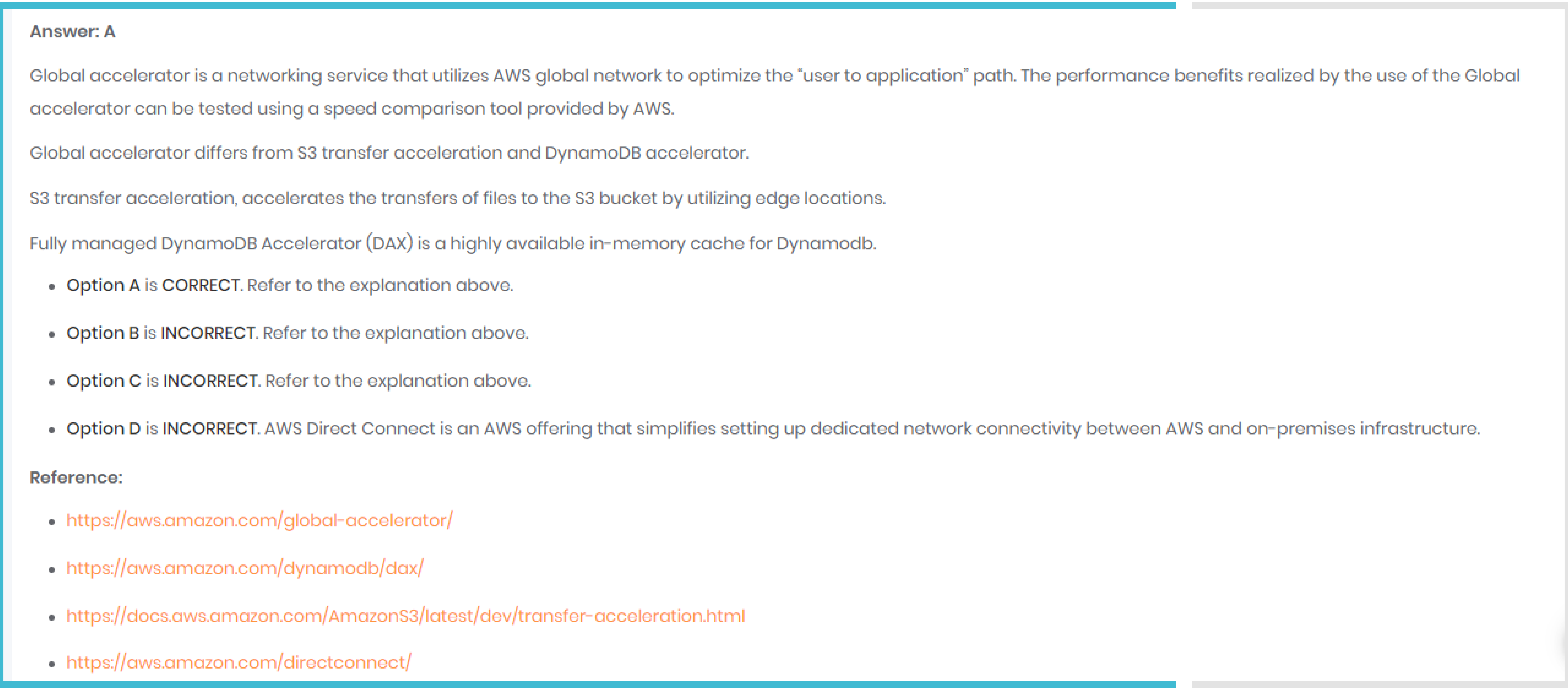


Answer: A

- **Option A** is **CORRECT**. AWS Data Sync is a simple and fast way to move huge amounts of data (hundreds of terabytes) between on-prem storage to S3, EFS, FSx.
- **Option B** is **INCORRECT**. AWS Direct Connect is an offering that helps run workloads that are heavy on bandwidth in AWS. AWS Direct Connect enables private and dedicated connections between the on-premises network and AWS. AWS Data Sync could be used over the internet or Direct Connect.
- **Option C** is **INCORRECT**. AWS Data Pipeline is a web service that facilitates data processing and movement between various AWS services (like compute and storage). Data pipeline also works well with data sources that are on-premise. In the given data migration scenario, data sync is a more apt choice.
- **Option D** is **INCORRECT**. AWS Migration Hub is a service that facilitates discovery of the existing applications and IT assets and provides a view to better plan and track application migrations.

Reference:

- https://aws.amazon.com/datasync/
- https://aws.amazon.com/directconnect/
- https://aws.amazon.com/datapipeline/
- https://aws.amazon.com/migration-hub/



Answer: A

Global accelerator is a networking service that utilizes AWS global network to optimize the "user to application" path. The performance benefits realized by the use of the Global accelerator can be tested using a speed comparison tool provided by AWS.

Global accelerator differs from S3 transfer acceleration and DynamoDB accelerator.

S3 transfer acceleration, accelerates the transfers of files to the S3 bucket by utilizing edge locations.

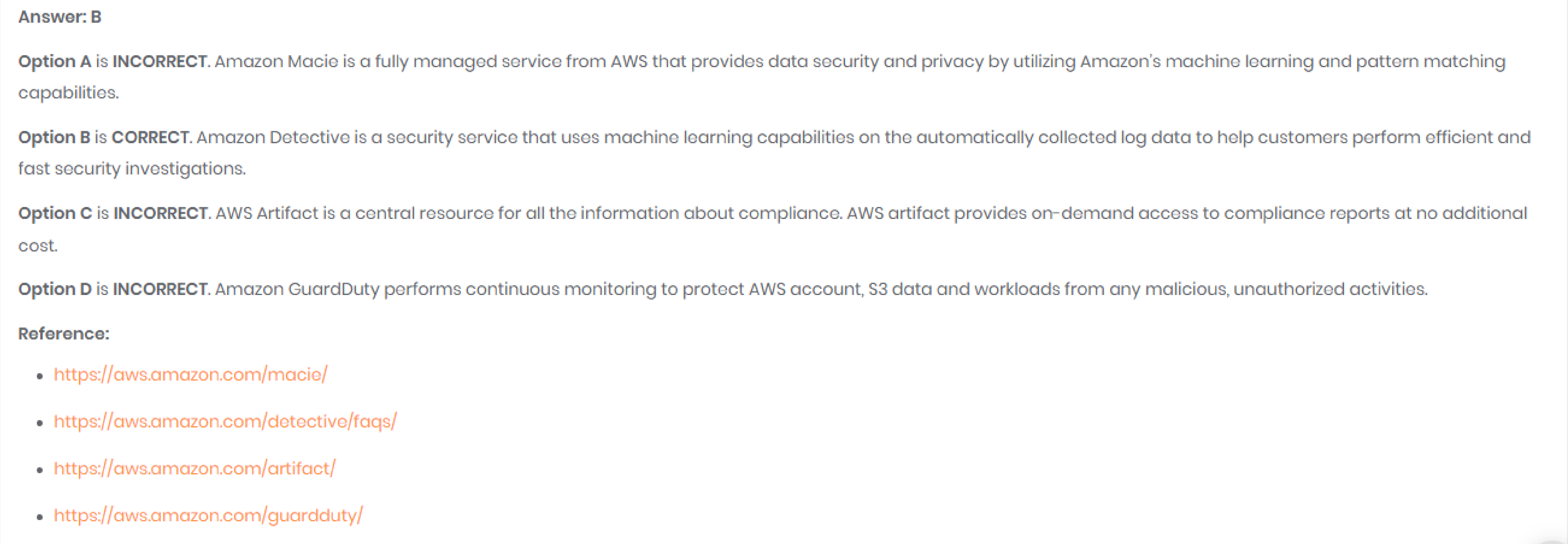
Fully managed DynamoDB Accelerator (DAX) is a highly available in-memory cache for Dynamodb.

- **Option A** is **CORRECT**. Refer to the explanation above.
- **Option B** is **INCORRECT**. Refer to the explanation above.
- **Option C** is **INCORRECT**. Refer to the explanation above.
- **Option D** is **INCORRECT**. AWS Direct Connect is an AWS offering that simplifies setting up dedicated network connectivity between AWS and on-premises infrastructure.

Reference:

- https://aws.amazon.com/global-accelerator/
- https://aws.amazon.com/dynamodb/dax/
- https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html
- https://aws.amazon.com/directconnect/

Ques No : 61



Answer: B

Option A is **INCORRECT**. Amazon Macie is a fully managed service from AWS that provides data security and privacy by utilizing Amazon's machine learning and pattern matching capabilities.

Option B is **CORRECT**. Amazon Detective is a security service that uses machine learning capabilities on the automatically collected log data to help customers perform efficient and fast security investigations.

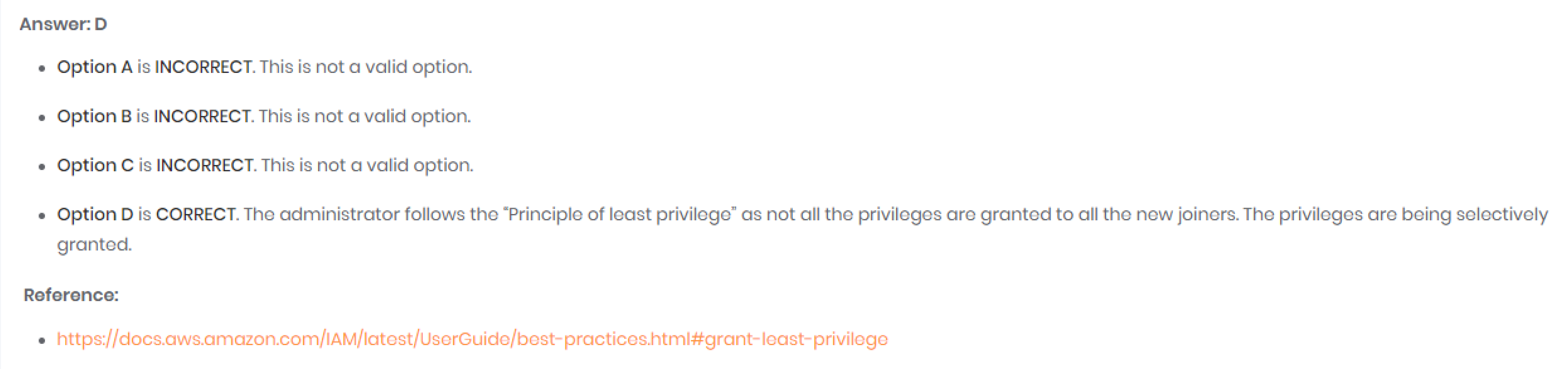
Option C is **INCORRECT**. AWS Artifact is a central resource for all the information about compliance. AWS artifact provides on-demand access to compliance reports at no additional cost.

Option D is **INCORRECT**. Amazon GuardDuty performs continuous monitoring to protect AWS account, S3 data and workloads from any malicious, unauthorized activities.

Reference:

- https://aws.amazon.com/macie/
- https://aws.amazon.com/detective/faqs/
- https://aws.amazon.com/artifact/
- https://aws.amazon.com/guardduty/

Ques No : 62



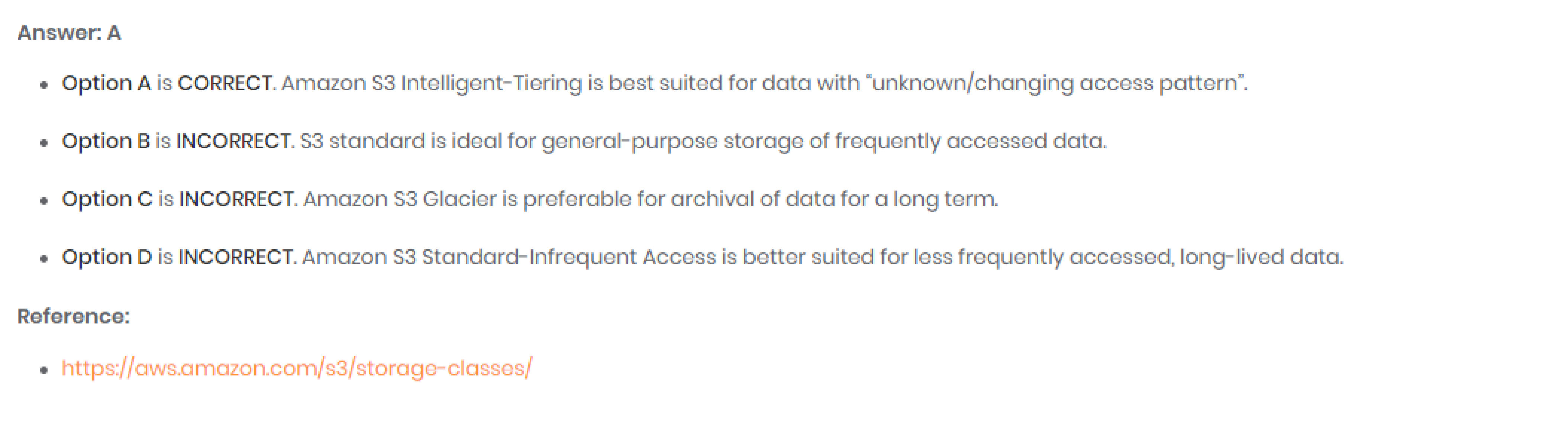
Answer: D

- **Option A** is **INCORRECT**. This is not a valid option.
- **Option B** is **INCORRECT**. This is not a valid option.
- **Option C** is **INCORRECT**. This is not a valid option.
- **Option D** is **CORRECT**. The administrator follows the "Principle of least privilege" as not all the privileges are granted to all the new joiners. The privileges are being selectively granted.

Reference:

- https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege

Ques No : 63

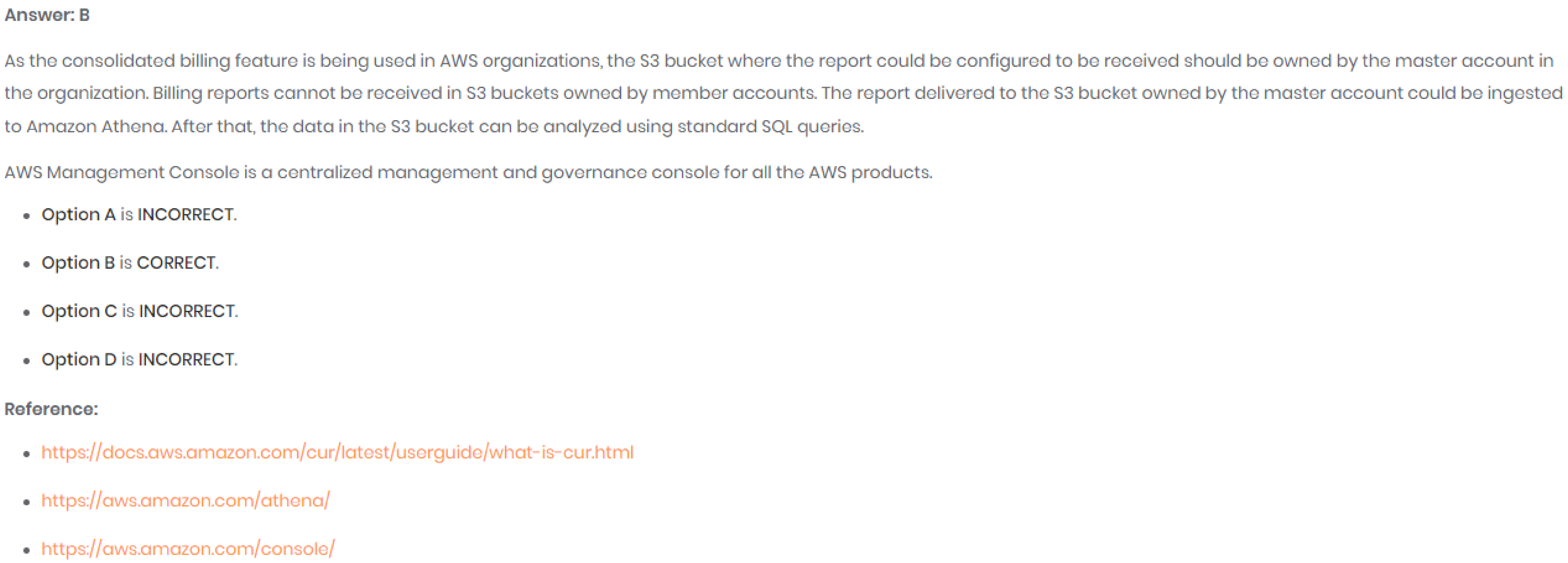


Answer: A

- **Option A** is **CORRECT**. Amazon S3 Intelligent-Tiering is best suited for data with “unknown/changing access pattern”.
- **Option B** is **INCORRECT**. S3 standard is ideal for general-purpose storage of frequently accessed data.
- **Option C** is **INCORRECT**. Amazon S3 Glacier is preferable for archival of data for a long term.
- **Option D** is **INCORRECT**. Amazon S3 Standard-Infrequent Access is better suited for less frequently accessed, long-lived data.

Reference:

- https://aws.amazon.com/s3/storage-classes/



Answer: B

As the consolidated billing feature is being used in AWS organizations, the S3 bucket where the report could be configured to be received should be owned by the master account in the organization. Billing reports cannot be received in S3 buckets owned by member accounts. The report delivered to the S3 bucket owned by the master account could be ingested to Amazon Athena. After that, the data in the S3 bucket can be analyzed using standard SQL queries.

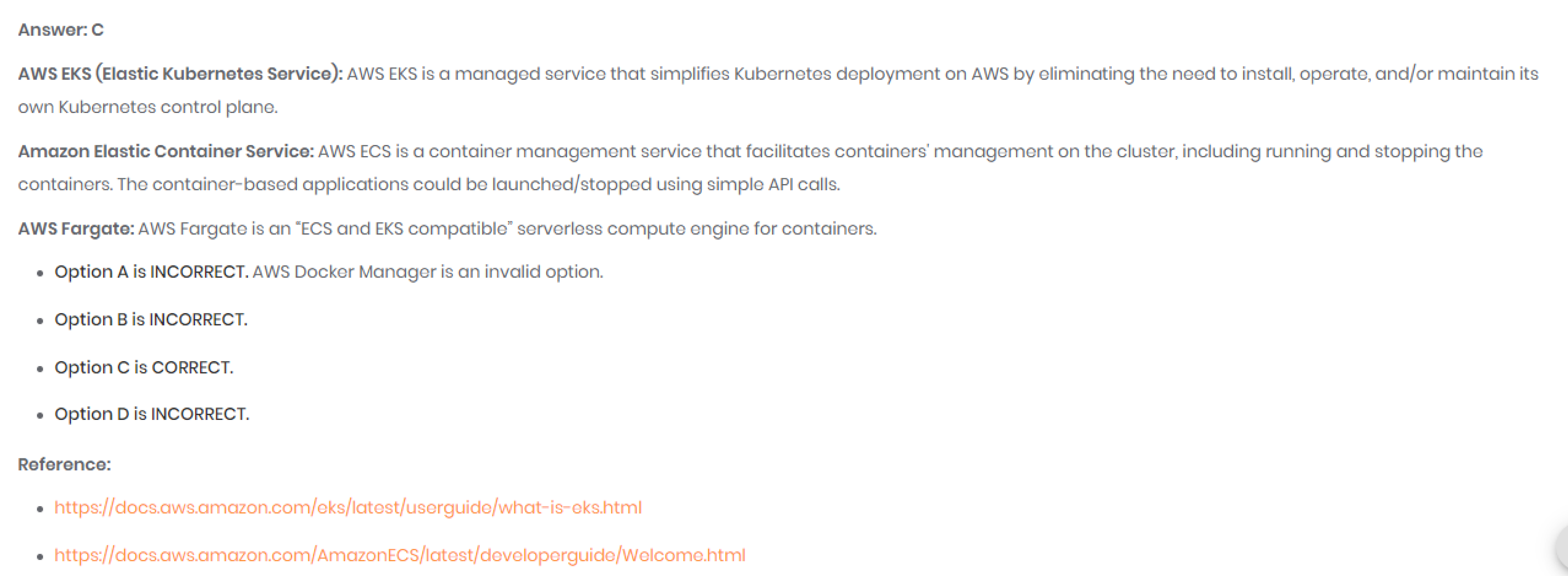
AWS Management Console is a centralized management and governance console for all the AWS products.

- Option A is INCORRECT.
- Option B is CORRECT.
- Option C is INCORRECT.
- Option D is INCORRECT.

Reference:

- https://docs.aws.amazon.com/cur/latest/userguide/what-is-cur.html
- https://aws.amazon.com/athena/
- https://aws.amazon.com/console/

Ques No : 65



Answer: C

AWS EKS (Elastic Kubernetes Service): AWS EKS is a managed service that simplifies Kubernetes deployment on AWS by eliminating the need to install, operate, and/or maintain its own Kubernetes control plane.

Amazon Elastic Container Service: AWS ECS is a container management service that facilitates containers' management on the cluster, including running and stopping the containers. The container-based applications could be launched/stopped using simple API calls.

AWS Fargate: AWS Fargate is an "ECS and EKS compatible" serverless compute engine for containers.

- **Option A is INCORRECT.** AWS Docker Manager is an invalid option.
- **Option B is INCORRECT.**
- **Option C is CORRECT.**
- **Option D is INCORRECT.**

Reference:

- https://docs.aws.amazon.com/eks/latest/userguide/what-is-eks.html
- https://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html

Thank you !!!