



Free Questions for CLF-C02

Shared by Lamb on 04-10-2023

For More Free Questions and Preparation Resources

[Check the Links on Last Page](#)



Question 1

Question Type: MultipleChoice

A company wants to receive a notification when a specific AWS cost threshold is reached.

Which AWS services or tools can the company use to meet this requirement? (Select TWO.)

Options:

- A- Amazon Simple Queue Service (Amazon SQS)
- B- AWS Budgets
- C- Cost Explorer
- D- Amazon CloudWatch
- E- AWS Cost and Usage Report

Answer:

B, D

Explanation:

AWS Budgets and Amazon CloudWatch are two AWS services or tools that the company can use to receive a notification when a specific AWS cost threshold is reached. AWS Budgets allows users to set custom budgets to track their costs and usage, and respond quickly to alerts received from email or Amazon Simple Notification Service (Amazon SNS) notifications if they exceed their threshold. Users can create cost budgets with fixed or variable target amounts, and configure their notifications for actual or forecasted spend. Users can also set up custom actions to run automatically or through an approval process when a budget target is exceeded. For example, users could automatically apply a custom IAM policy that denies them the ability to provision additional resources within an account. Amazon CloudWatch is a service that monitors applications, responds to performance changes, optimizes resource use, and provides insights into operational health. Users can use CloudWatch to collect and track metrics, which are variables they can measure for their resources and applications. Users can create alarms that watch metrics and send notifications or automatically make changes to the resources they are monitoring when a threshold is breached. Users can use CloudWatch to monitor their AWS costs and usage by creating billing alarms that send notifications when their estimated charges exceed a specified threshold amount. Users can also use CloudWatch to monitor their Reserved Instance (RI) or Savings Plans utilization and coverage, and receive notifications when they fall below a certain level.

References: [Cloud Cost And Usage Budgets - AWS Budgets](#), [What is Amazon CloudWatch?](#), [Creating a billing alarm - Amazon CloudWatch](#)

Question 2

Question Type: MultipleChoice

Which cloud concept is demonstrated by using AWS Compute Optimizer?

Options:

- A- Security validation
- B- Rightsizing
- C- Elasticity
- D- Global reach

P2P
exams

Answer:

B

Explanation:

Rightsizing is the cloud concept that is demonstrated by using AWS Compute Optimizer. Rightsizing is the process of adjusting the type and size of your cloud resources to match the optimal performance and cost for your workloads. AWS Compute Optimizer is a service that analyzes the configuration and utilization metrics of your AWS resources, such as Amazon EC2 instances, Amazon EBS volumes, AWS Lambda functions, and Amazon ECS services on AWS Fargate. It reports whether your resources are optimal, and generates optimization recommendations to reduce the cost and improve the performance of your workloads. AWS Compute Optimizer uses machine learning to analyze your historical utilization data and compare it with the most cost-effective AWS alternatives. You can use the recommendations to evaluate the trade-offs between cost and performance, and decide when to move or resize your resources to achieve the best results. References: Workload Rightsizing - AWS Compute Optimizer - AWS, What is AWS Compute Optimizer? - AWS Compute Optimizer

Question 3

Question Type: MultipleChoice

A company wants to create a globally accessible ecommerce platform for its customers. The company wants to use a highly available and scalable DNS web service to connect users to the platform.

Which AWS service will meet these requirements?

Options:

- A- Amazon EC2
- B- Amazon VPC
- C- Amazon Route 53
- D- Amazon RDS

Answer:

C

Explanation:

Amazon Route 53 is a highly available and scalable Domain Name System (DNS) web service that can route internet traffic to the company's ecommerce platform¹. Route 53 can also register domain names, check the health of resources, and provide global DNS features². Route 53 can connect users to the platform by translating human-readable names like www.example.com into the numeric IP addresses that computers use to communicate with each other². References: ¹: [Amazon Route 53 | DNS Service | AWS](#); ²: [What is Amazon Route 53? - Amazon Route 53](#)

Question 4

Question Type: MultipleChoice

A company wants to set up its workloads to perform their intended functions and recover quickly from failure. Which pillar of the AWS Well-Architected Framework aligns with these goals?

Options:

- A- Performance efficiency
- B- Sustainability
- C- Reliability
- D- Security

Answer:

C

Explanation:

Understanding the Reliability Pillar: The Reliability pillar of the AWS Well-Architected Framework focuses on the ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues.

Key Concepts of Reliability:

Foundations: Ensure a solid foundation on which to build, including AWS account management, limits, and networking.

Change Management: Manage changes in automation to ensure systems remain reliable during modifications.

Failure Management: Design systems to detect failures and automatically recover from them.

How to Align with Reliability Pillar:

Implement Multi-AZ Deployments: Deploy applications across multiple Availability Zones to ensure fault tolerance.

Use Auto Scaling: Automatically adjust resources to maintain system performance during demand fluctuations.

Monitor and Respond: Implement monitoring and alerting mechanisms using services like CloudWatch to detect and respond to issues proactively.

References:

[AWS Well-Architected Framework: Reliability Pillar](#)

Question 5

Question Type: MultipleChoice

Which maintenance task is the customer's responsibility, according to the AWS shared responsibility model?

Options:

- A- Physical connectivity among Availability Zones
- B- Network switch maintenance
- C- Hardware updates and firmware patches
- D- Amazon EC2 updates and security patches

Answer:

D

Explanation:

According to the AWS shared responsibility model, customers are responsible for managing their data, applications, operating systems, security groups, and other aspects of their AWS environment. This includes installing updates and security patches of the guest operating system and any application software or utilities installed by the customer on the instances. AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud, such as data centers, hardware, software, networking, and facilities. This includes the physical connectivity among Availability Zones, the network switch maintenance, and the hardware updates and firmware patches. Therefore, option D is the correct answer, and options A, B, and C are AWS responsibilities, not customer responsibilities. References: : AWS Well-Architected Framework - Elasticity; : Reactive Systems on AWS - Elastic

Question 6

Question Type: MultipleChoice

To assist companies with Payment Card Industry Data Security Standard (PCI DSS) compliance in the cloud. AWS provides:

Options:

- A- physical inspections of data centers by appointment.
- B- required PCI compliance certifications for any application running on AWS.
- C- an AWS Attestation of Compliance (AOC) report for specific AWS services.
- D- professional PCI compliance services.

Answer:

C

Explanation:

AWS provides an Attestation of Compliance (AOC) report for specific AWS services to assist companies in achieving Payment Card Industry Data Security Standard (PCI DSS) compliance in

the cloud. This report demonstrates that AWS services meet the necessary PCI DSS requirements. AWS does not offer physical inspections of data centers by appointment, nor does it provide certifications for any application running on AWS. Additionally, AWS does not provide professional PCI compliance services; companies must manage their PCI compliance in their environment.

Question 7

Question Type: MultipleChoice

Which of the following is a fully managed MySQL-compatible database?

Options:

- A- Amazon S3
- B- Amazon DynamoDB
- C- Amazon Redshift
- D- Amazon Aurora

Answer:

D

Explanation:

Amazon Aurora is a fully managed MySQL-compatible database that combines the performance and availability of traditional enterprise databases with the simplicity and cost-effectiveness of open-source databases. Amazon Aurora is part of the Amazon Relational Database Service (Amazon RDS) family, which means it inherits the benefits of a fully managed service, such as automated backups, patches, scaling, monitoring, and security. Amazon Aurora also offers up to five times the throughput of standard MySQL, as well as high availability, durability, and fault tolerance with up to 15 read replicas, cross-Region replication, and self-healing storage. Amazon Aurora is compatible with the latest versions of MySQL, as well as PostgreSQL, and supports various features and integrations that enhance its functionality and usability.

References: [Amazon Aurora](#), [Amazon RDS](#), [AWS --- Amazon Aurora Overview](#)

Question 8

Question Type: MultipleChoice

A company has a MySQL database running on a single Amazon EC2 instance. The company now requires higher availability in the event of an outage.

Which set of tasks would meet this requirement?

Options:

- A- Add an Application Load Balancer in front of the EC2 instance.
- B- Configure EC2 Auto Recovery to move the instance to another Availability Zone.
- C- Migrate to Amazon RDS and enable Multi-AZ.
- D- Enable termination protection for the EC2 instance to avoid outages.

Answer:

C

Explanation:

The set of tasks that would meet the requirement of having higher availability for a MySQL database running on a single Amazon EC2 instance is to migrate to Amazon RDS and enable Multi-AZ. Amazon RDS is a fully managed relational database service that supports MySQL and other popular database engines. By enabling Multi-AZ, users can have a primary database in one Availability Zone and a synchronous standby replica in another Availability Zone. In case of a planned or unplanned outage of the primary database, Amazon RDS automatically fails over to the standby replica with minimal disruption. Adding an Application Load Balancer in front of the EC2 instance, configuring EC2 Auto Recovery to move the instance to another Availability Zone, or enabling termination protection for the EC2 instance would not provide higher availability for the database, as they do not address the single point of failure or data replication issues.

Question 9

Question Type: MultipleChoice

A company needs to track the activity in its AWS accounts, and needs to know when an API call is made against its AWS resources. Which AWS tool or service can be used to meet these requirements?

Options:

- A- Amazon CloudWatch
- B- Amazon Inspector
- C- AWS CloudTrail
- D- AWS IAM

Answer:

C

Explanation:

AWS CloudTrail is the service that can be used to meet these requirements. AWS CloudTrail is a service that records AWS API calls for your account and delivers log files to you. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service¹. You can use CloudTrail to track the activity in your AWS accounts, such as who made an API call, when it was made, and what resources were affected. You can also use CloudTrail to monitor the compliance, security, and governance of your AWS environment². The other services are not designed to track the activity and API calls in your AWS accounts. Amazon CloudWatch is a service that monitors and collects metrics, logs, and events from your AWS resources and applications. You can use CloudWatch to set alarms, visualize data, and automate actions based on predefined thresholds or rules³. Amazon Inspector is a service that helps you improve the security and compliance of your applications running on AWS. Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices⁴. AWS IAM is a service that enables you to manage access to AWS services and resources securely. IAM allows you to create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. References: AWS CloudTrail, AWS CloudTrail -- Capture AWS API Activity, Amazon CloudWatch, Amazon Inspector, [AWS IAM]

Question 10

Question Type: MultipleChoice

A company needs a graph database service that is scalable and highly available.

Which AWS service meets these requirements?

Options:

- A- Amazon Aurora
- B- Amazon Redshift
- C- Amazon DynamoDB
- D- Amazon Neptune

Answer:

D

Explanation:

The AWS service that meets the requirements of providing a graph database service that is scalable and highly available is Amazon Neptune. Amazon Neptune is a fast, reliable, and fully managed graph database service that supports property graph and RDF graph models. Amazon Neptune is designed to store billions of relationships and query the graph with milliseconds latency. Amazon Neptune also offers high availability and durability by replicating six copies of the data across three Availability Zones and continuously backing up the data to Amazon S3. Amazon Aurora, Amazon Redshift, and Amazon DynamoDB are other AWS services that provide relational or non-relational database solutions, but they do not support graph database models.

Question 11

Question Type: MultipleChoice

Which AWS service or tool can be used to set up a firewall to control traffic going into and coming out of an Amazon VPC subnet?

Options:

- A- Security group
- B- AWS WAF
- C- AWS Firewall Manager
- D- Network ACL

Answer:

D

Explanation:

A network ACL (NACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You can create a network ACL and associate it with a subnet to apply rules that allow or deny traffic to or from the subnet. Network ACLs are stateless, meaning that they evaluate the source and destination IP addresses for both inbound and outbound traffic. You can also use network ACLs to block IP address ranges that are known to be malicious¹².

The other options are not AWS services or tools that can be used to set up a firewall to control traffic going into and coming out of an Amazon VPC subnet. Security groups are another layer of security for your VPC that act as a firewall for your EC2 instances. Security groups are stateful, meaning that they automatically allow return traffic for allowed inbound traffic. Security groups can only filter traffic based on protocols, ports, and source or destination IP addresses, not on IP ranges³. AWS WAF is a web application firewall that helps protect your web applications from common web exploits. AWS WAF can filter web requests based on rules that you define, such as IP addresses, HTTP headers, HTTP body, or URI strings. AWS WAF does not apply to non-web traffic or to traffic within a VPC⁴. AWS Firewall Manager is a service that helps you centrally configure and manage firewall rules across your accounts and resources in AWS Organizations. You can use Firewall Manager to apply AWS WAF rules, AWS Network Firewall policies, and Amazon VPC security groups across your AWS accounts. AWS Firewall Manager does not provide a firewall service itself, but rather helps you manage other firewall services



To Get Premium Files for CLF-C02 Visit

<https://www.p2pexams.com/products/clf-c02>

For More Free Questions Visit

<https://www.p2pexams.com/amazon/pdf/clf-c02>

20%
DISCOUNT

P2P
exams