



CLF-C02^{Q&As}

AWS Certified Cloud Practitioner

Pass Amazon CLF-C02 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/clf-c02.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

Which of the following is a characteristic of the AWS account root user?

- A. The root user is the only user that can be configured with multi-factor authentication (MFA).
- B. The root user is the only user that can access the AWS Management Console.
- C. The root user is the first sign-in identity that is available when an AWS account is created.
- D. The root user has a password that cannot be changed.

Correct Answer: C

The AWS account root user is the first sign-in identity that is available when an AWS account is created. It has complete access to all AWS services and resources in the account. The root user email address and password are the same credentials that are used to sign in to the AWS Management Console⁴. The root user should be used only to perform a few account and service management tasks. For day-to-day tasks, it is recommended to use AWS Identity and Access Management (IAM) users or roles instead.

QUESTION 2

A company has teams that have different job roles and responsibilities. The company's employees often change teams. The company needs to manage permissions for the employees so that the permissions are appropriate for the job responsibilities. Which IAM resource should the company use to meet this requirement with the LEAST operational overhead?

- A. IAM user groups
- B. IAM roles
- C. IAM instance profiles
- D. IAM policies for individual users

Correct Answer: B

QUESTION 3

Which tasks are customer responsibilities, according to the AWS shared responsibility model? (Select TWO.)

- A. Configure the AWS provided security group firewall.
- B. Classify company assets in the AWS Cloud.
- C. Determine which Availability Zones to use for Amazon S3 buckets.
- D. Patch or upgrade Amazon DynamoDB.
- E. Select Amazon EC2 instances to run AWS Lambda on.



F. AWS Config

Correct Answer: AB

According to the AWS shared responsibility model, the customer is responsible for security in the cloud, which includes the tasks of configuring the AWS provided security group firewall and classifying company assets in the AWS Cloud. A security group is a virtual firewall that controls the inbound and outbound traffic for one or more EC2 instances. The customer must configure the security group rules to allow or deny traffic based on protocol, port, or source and destination IP address² Classifying company assets in the AWS Cloud means identifying the types, categories, and sensitivity levels of the data and resources that the customer stores and processes on AWS. The customer must also determine the applicable compliance requirements and regulations that apply to their assets, and implement the appropriate security controls and measures to protect them

QUESTION 4

Which encryption types can be used to protect objects at rest in Amazon S3? (Select TWO.)

- A. Server-side encryption with AmazonS3 managed encryption keys (SSE-S3)
- B. Server-side encryption with AWS KMSmanaged keys (SSE-KMS)
- C. TLS
- D. SSL
- E. Transparent Data Encryption (TDE)

Correct Answer: AB

Server-side encryption with Amazon S3 managed encryption keys (SSE-S3) and server-side encryption with AWS KMS managed keys (SSE-KMS) are the encryption types that can be used to protect objects at rest in Amazon S3. Server-side encryption means that Amazon S3 encrypts the objects before saving them on disks and decrypts them when they are downloaded. SSE-S3 uses one master key per bucket that is managed by Amazon S3. SSE-KMS uses a customer master key (CMK) that is stored in AWS Key Management Service (AWS KMS) and provides additional benefits, such as audit trails and key rotation. For more information, see [Protecting Data Using Server-Side Encryption](#) and [Protecting Data Using Encryption](#).

QUESTION 5

Which option is an AWS Cloud Adoption Framework (AWS CAF) foundational capability for the operations perspective?

- A. Performance and capacity management
- B. Application portfolio management
- C. Identity and access management
- D. Product management

Correct Answer: C

Identity and access management is one of the foundational capabilities for the operations perspective of the AWS Cloud Adoption Framework (AWS CAF). It involves managing the identities, roles, permissions, and credentials of users and



systems that interact with AWS resources. Performance and capacity management is a capability for the platform perspective. Application portfolio management is a capability for the business perspective. Product management is a capability for the governance perspective.

[CLF-C02 VCE Dumps](#)

[CLF-C02 Study Guide](#)

[CLF-C02 Exam Questions](#)