

## CLF-C02<sup>Q&As</sup>

AWS Certified Cloud Practitioner

**Pass Amazon CLF-C02 Exam with 100% Guarantee**

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

<https://www.leads4pass.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 describes some of the core functionality of Amazon S3?

- A. Amazon S3 is a high-performance block storage service that is designed for use with Amazon EC2.
- B. Amazon S3 is an object storage service that provides high-level performance, security, scalability, and data availability.
- C. Amazon S3 is a fully managed, highly reliable, and scalable file storage system that is accessible over the industry-standard SMB protocol.
- D. Amazon S3 is a scalable, fully managed elastic NFS for use with AWS Cloud services and on-premises resources.

Correct Answer: B

---

**QUESTION 2**

A company wants to design a reliable web application that is hosted on Amazon EC2.

Which approach will achieve this goal?

- A. Launch large EC2 instances in the same Availability Zone.
- B. Spread EC2 instances across more than one security group.
- C. Spread EC2 instances across more than one Availability Zone.
- D. Use an Amazon Machine Image (AMI) from AWS Marketplace.

Correct Answer: C

Explanation: The approach that will achieve the goal of designing a reliable web application that is hosted on Amazon EC2 is to spread EC2 instances across more than one Availability Zone. An Availability Zone is a physically isolated location within an AWS Region that has its own power, cooling, and network connectivity. By spreading EC2 instances across multiple Availability Zones, users can increase the fault tolerance and availability of their web applications, as well as reduce latency for end users<sup>2</sup>. Launching large EC2 instances in the same Availability Zone, spreading EC2 instances across more than one security group, or using an Amazon Machine Image (AMI) from AWS Marketplace are not sufficient to ensure reliability, as they do not provide redundancy or resilience in case of an outage in one Availability Zone.

---

**QUESTION 3**

Which option is an AWS Cloud Adoption Framework (AWS CAF) platform perspective capability?

- A. Data architecture
- B. Data protection
- C. Data governance

D. Data science

Correct Answer: A

<https://abhi0751.medium.com/aws-cloud-adoption-framework-aws-caf-a512b89dbcba>

---

#### QUESTION 4

Which task requires the use of AWS account root user credentials?

- A. The deletion of IAM users
- B. The change to a different AWS Support plan
- C. The creation of an organization in AWS Organizations
- D. The deletion of Amazon EC2 instances

Correct Answer: C

Explanation: The creation of an organization in AWS Organizations requires the use of AWS account root user credentials. The AWS account root user is the email address that was used to create the AWS account. The root user has complete access to all AWS services and resources in the account, and can perform sensitive tasks such as changing the account settings, closing the account, or creating an organization. The root user credentials should be used sparingly and securely, and only for tasks that cannot be performed by IAM users or roles4

---

#### QUESTION 5

A developer has been hired by a large company and needs AWS credentials.

Which are security best practices that should be followed? (Select TWO.)

- A. Grant the developer access to only the AWS resources needed to perform the job.
- B. Share the AWS account root user credentials with the developer.
- C. Add the developer to the administrator's group in AWS IAM.
- D. Configure a password policy that ensures the developer's password cannot be changed.
- E. Ensure the account password policy requires a minimum length.

Correct Answer: AE

The security best practices that should be followed are A and E. A. Grant the developer access to only the AWS resources needed to perform the job. This is an example of the principle of least privilege, which means giving the minimum permissions necessary to achieve a task. This reduces the risk of unauthorized access, data leakage, or accidental damage to AWS resources. You can use AWS Identity and Access Management (IAM) to create users, groups, roles, and policies that grant fine-grained access to AWS resources12.

E. Ensure the account password policy requires a minimum length. This is a basic security measure that helps prevent brute-force attacks or guessing of passwords. A longer password is harder to crack than a shorter one. You can use IAM to configure a password policy that enforces a minimum password length, as well as other requirements such as

complexity, expiration, and history<sup>34</sup>.

B. Share the AWS account root user credentials with the developer. This is a bad practice that should be avoided. The root user has full access to all AWS resources and services, and can perform sensitive actions such as changing billing information, closing the account, or deleting all resources. Sharing the root user credentials exposes your account to potential compromise or misuse. You should never share your root user credentials with anyone, and use them only for account administration tasks<sup>5</sup>. C. Add the developer to the administrator's group in IAM. This is also a bad practice that should be avoided. The administrator's group has full access to all AWS resources and services, which is more than what a developer needs to perform their job. Adding the developer to the administrator's group violates the principle of least privilege and increases the risk of unauthorized access, data leakage, or accidental damage to AWS resources. You should create a custom group for the developer that grants only the necessary permissions for their role<sup>12</sup>.

D. Configure a password policy that ensures the developer's password cannot be changed. This is another bad practice that should be avoided. Preventing the developer from changing their password reduces their ability to protect their credentials and comply with security policies. For example, if the developer's password is compromised, they cannot change it to prevent further unauthorized access. Or if the company requires periodic password rotation, they cannot update their password to meet this requirement. You should allow the developer to change their password as needed, and enforce a password policy that sets reasonable rules for password management<sup>34</sup>.

[Latest CLF-C02 Dumps](#)

[CLF-C02 Practice Test](#)

[CLF-C02 Exam Questions](#)