Free Questions for CLF-C02 by dumpssheet

Shared by Hudson on 18-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A newly created 1AM user has no 1AM policy attached.

What will happen when the user logs in and attempts to view the AWS resources in the account?

Options:

A) All AWS services will be read-only access by default.

B) Access to all AWS resources will be denied.

C) Access to the AWS billing services will be allowed.

D) Access to AWS resources will be allowed through the AWS CLL

Answer:

B

Explanation:

Access to all AWS resources will be denied if a newly created IAM user has no IAM policy attached and logs in and attempts to view the AWS resources in the account. IAM policies are the way to grant permissions to IAM users, groups, and roles to access and manage AWS resources. By default, IAM users have no permissions, unless they are explicitly granted by an IAM policy. Therefore, a newly created IAM user without any IAM policy attached will not be able to view or perform any actions on the AWS resources in the account. Access to the AWS billing services and AWS CLI will also be denied, unless the user has the necessary permissions.

Question 2

Question Type: MultipleChoice

A company is setting up AWS Identity and Access Management (1AM) on an AWS account.

Which recommendation complies with 1AM security best practices?

Options:

A) Use the account root user access keys for administrative tasks.

B) Grant broad permissions so that all company employees can access the resources they need.

C) Turn on multi-factor authentication (MFA) for added security during the login process.

D) Avoid rotating credentials to prevent issues in production applications.

Answer:

C

Explanation:

C is correct because turning on multi-factor authentication (MFA) for added security during the login process is one of the IAM security best practices recommended by AWS. MFA adds an extra layer of protection on top of the user name and password, making it harder for attackers to access the AWS account. A is incorrect because using the account root user access keys for administrative tasks is not a good practice, as the root user has full access to all the resources in the AWS account and can cause irreparable damage if compromised. AWS recommends creating individual IAM users with the least privilege principle and using roles for applications that run on Amazon EC2 instances. B is incorrect because granting broad permissions so that all company employees can access the resources they need is not a good practice, as it increases the risk of unauthorized or accidental actions on the AWS resources. AWS recommends granting only the permissions that are required to perform a task and using groups to assign permissions to IAM users. D is incorrect because avoiding rotating credentials to prevent issues in production applications is not a good practice, as it increases the risk of credential leakage or compromise. AWS recommends rotating credentials regularly and using temporary security credentials from AWS STS when possible.

Question 3

Question Type: **MultipleChoice**

Which of the following actions are controlled with AWS Identity and Access Management (1AM)? (Select TWO.)

Options:

A) Control access to AWS service APIs and to other specific resources.

B) Provide intelligent threat detection and continuous monitoring.

C) Protect the AWS environment using multi-factor authentication (MFA).

D) Grant users access to AWS data centers.

E) Provide firewall protection for applications from common web attacks.

Answer:

A, C

Explanation:

AWS Identity and Access Management (IAM) is a service that enables you to manage access to AWS services and resources securely. You can use IAM to perform the following actions:

Control access to AWS service APIs and to other specific resources: You can create users, groups, roles, and policies that define who can access which AWS resources and how.You can also use IAM to grant temporary access to users or applications that need to perform certain tasks on your behalf3

Protect the AWS environment using multi-factor authentication (MFA): You can enable MFA for your IAM users and root user to add an extra layer of security to your AWS account.MFA requires users to provide a unique authentication code from an approved device or SMS text message, in addition to their user name and password, when they sign in to AWS4

Question 4

Question Type: **MultipleChoice**

A newly created 1AM user has no 1AM policy attached.

What will happen when the user logs in and attempts to view the AWS resources in the account?

Options:

A) All AWS services will be read-only access by default.

B) Access to all AWS resources will be denied.

C) Access to the AWS billing services will be allowed.

D) Access to AWS resources will be allowed through the AWS CLL

Answer:

B

Explanation:

Access to all AWS resources will be denied if a newly created IAM user has no IAM policy attached and logs in and attempts to view the AWS resources in the account. IAM policies are the way to grant permissions to IAM users, groups, and roles to access and manage AWS resources. By default, IAM users have no permissions, unless they are explicitly granted by an IAM policy. Therefore, a newly created IAM user without any IAM policy attached will not be able to view or perform any actions on the AWS resources in the account. Access to the AWS billing services and AWS CLI will also be denied, unless the user has the necessary permissions.

Question 5

Question Type: MultipleChoice

Which of the following actions are controlled with AWS Identity and Access Management (1AM)? (Select TWO.)

Options:

A) Control access to AWS service APIs and to other specific resources.

B) Provide intelligent threat detection and continuous monitoring.

C) Protect the AWS environment using multi-factor authentication (MFA).

D) Grant users access to AWS data centers.

E) Provide firewall protection for applications from common web attacks.

Answer:

A, C

Explanation:

AWS Identity and Access Management (IAM) is a service that enables you to manage access to AWS services and resources securely. You can use IAM to perform the following actions:

Control access to AWS service APIs and to other specific resources: You can create users, groups, roles, and policies that define who can access which AWS resources and how.You can also use IAM to grant temporary access to users or applications that need to perform certain tasks on your behalf3

Protect the AWS environment using multi-factor authentication (MFA): You can enable MFA for your IAM users and root user to add an extra layer of security to your AWS account.MFA requires users to provide a unique authentication code from an approved device or SMS text message, in addition to their user name and password, when they sign in to AWS4

Question 6

Question Type: MultipleChoice

A company is setting up AWS Identity and Access Management (1AM) on an AWS account.

Which recommendation complies with 1AM security best practices?

Options:

A) Use the account root user access keys for administrative tasks.

B) Grant broad permissions so that all company employees can access the resources they need.

C) Turn on multi-factor authentication (MFA) for added security during the login process.

D) Avoid rotating credentials to prevent issues in production applications.

Answer:

C

Explanation:

C is correct because turning on multi-factor authentication (MFA) for added security during the login process is one of the IAM security best practices recommended by AWS. MFA adds an extra layer of protection on top of the user name and password, making it harder for attackers to access the AWS account. A is incorrect because using the account root user access keys for administrative tasks is not a good practice, as the root user has full access to all the resources in the AWS account and can cause irreparable damage if compromised. AWS recommends creating individual IAM users with the least privilege principle and using roles for applications that run on Amazon EC2 instances. B is incorrect because granting broad permissions so that all company employees can access the resources they need is not a good practice, as it increases the risk of unauthorized or accidental actions on the AWS resources. AWS recommends granting only the permissions that are required to perform a task and using groups to assign permissions to IAM users. D is incorrect because avoiding rotating credentials to prevent issues in production applications is not a good practice, as it increases the risk of credential leakage or compromise. AWS recommends rotating credentials regularly and using temporary security credentials from AWS STS when possible.