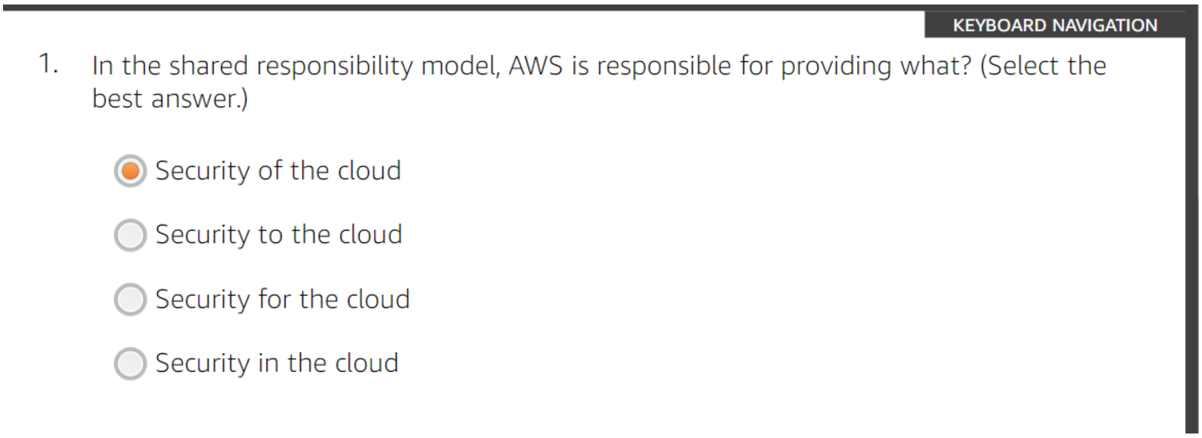
Module 4 Answer



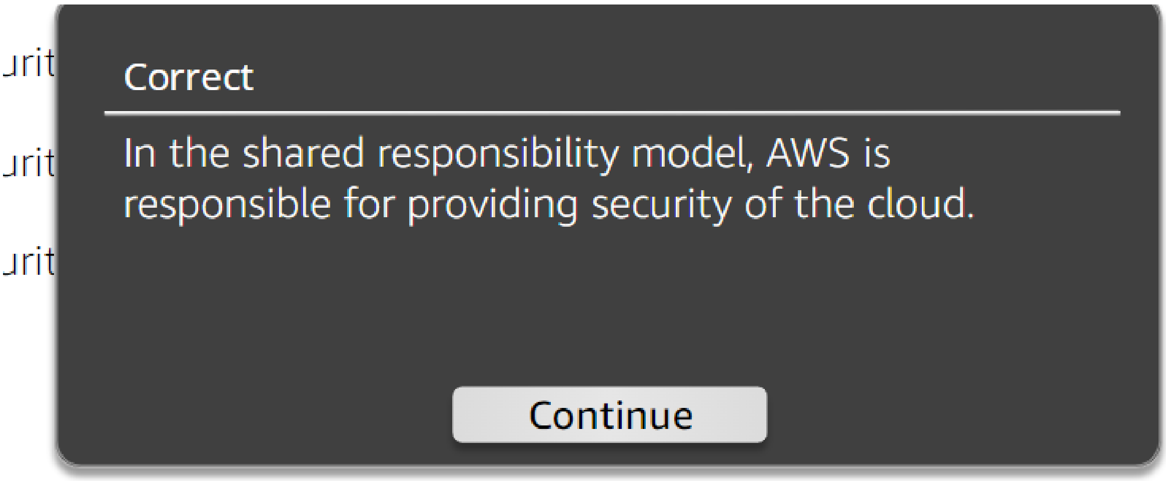
1. In the shared responsibility model, AWS is responsible for providing what? (Select the best answer.)

● Security of the cloud

○ Security to the cloud

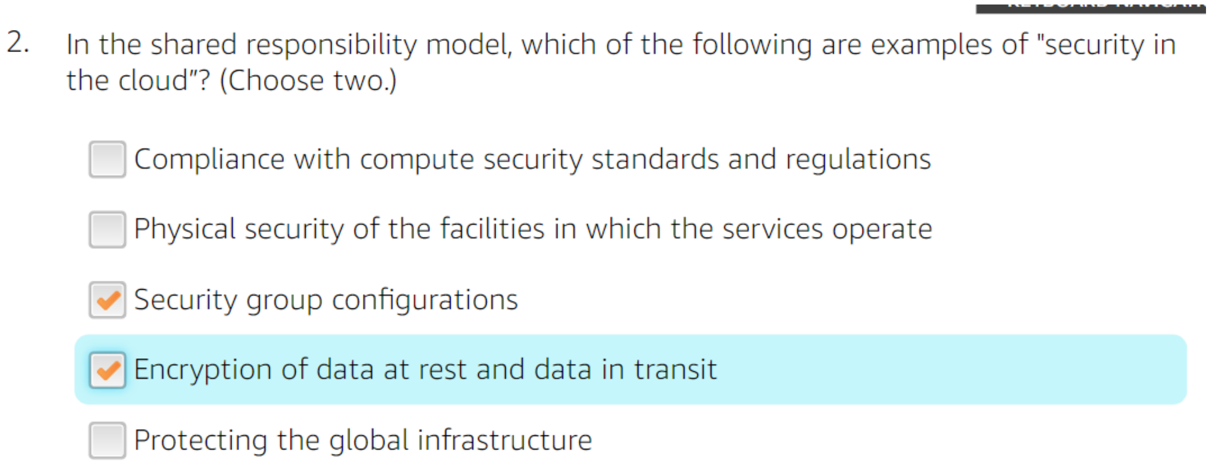
○ Security for the cloud

○ Security in the cloud



Correct

In the shared responsibility model, AWS is responsible for providing security of the cloud.



2. In the shared responsibility model, which of the following are examples of "security in the cloud"? (Choose two.)

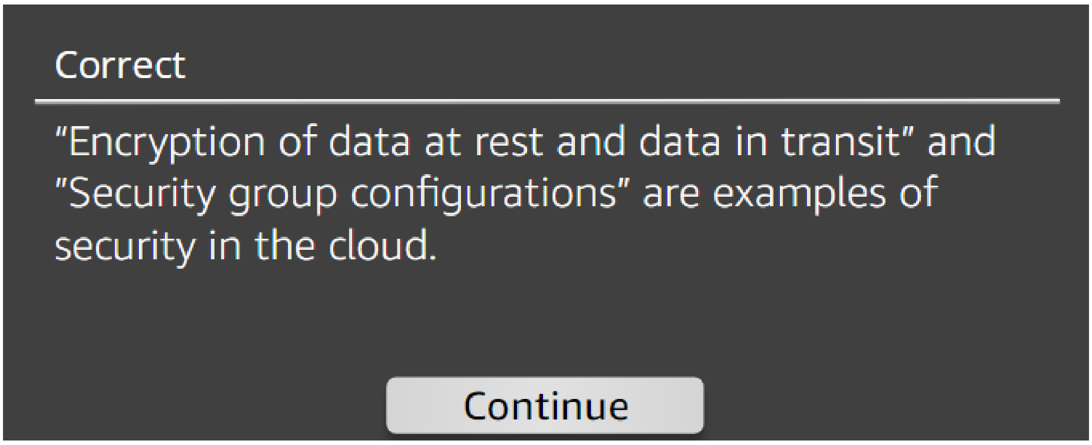
☐ Compliance with compute security standards and regulations

☐ Physical security of the facilities in which the services operate

☑ Security group configurations

☑ Encryption of data at rest and data in transit

☐ Protecting the global infrastructure



Correct

“Encryption of data at rest and data in transit” and ”Security group configurations” are examples of security in the cloud.

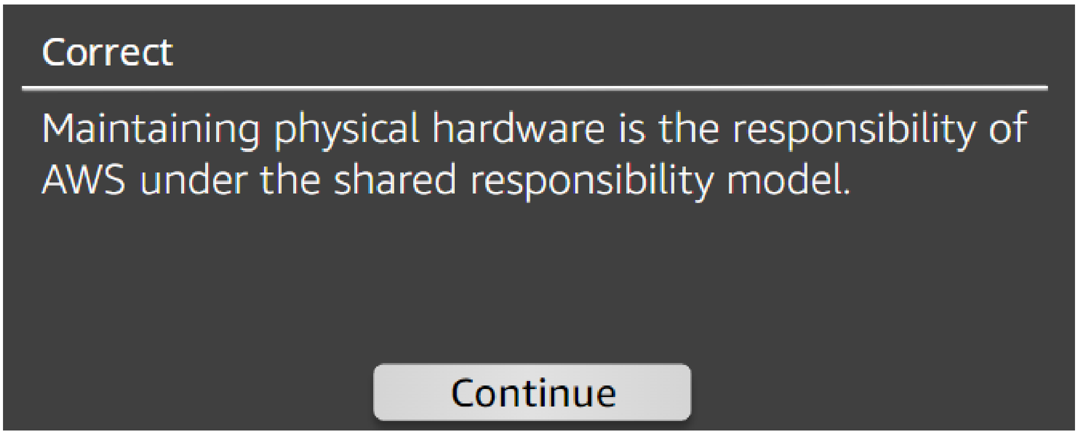
3. Which of the following is the responsibility of AWS under the AWS shared responsibility model? (Select the best answer.)

○ Configuring third-party applications

● Maintaining physical hardware

○ Security application access and data

○ Managing custom Amazon Machine Images (AMIs)



Correct

Maintaining physical hardware is the responsibility of AWS under the shared responsibility model.

4. When creating an AWS Identity and Access Management (IAM) policy, what are the two types of access that can be granted to a user? (Choose two.)

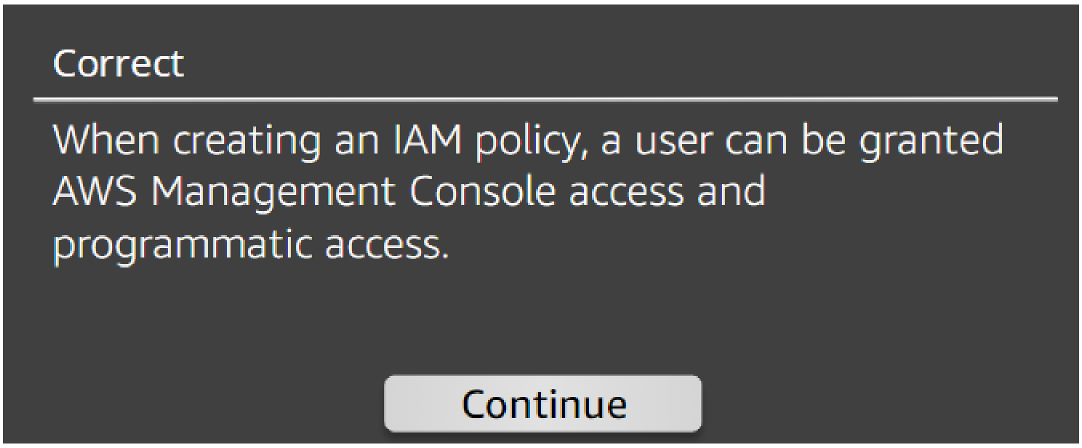
□ Institutional access

□ Authorized access

☑ Programmatic access

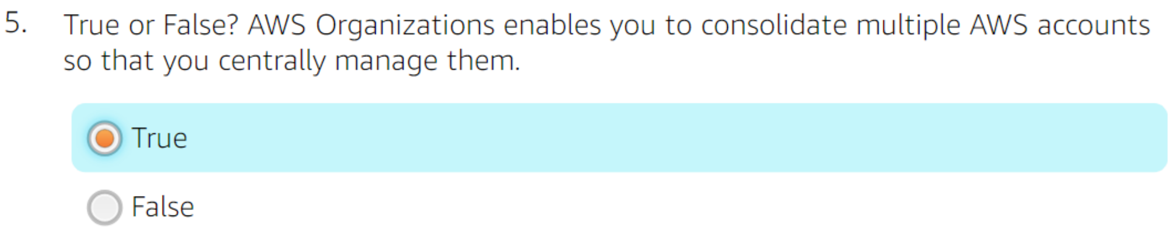
☑ AWS Management Console access

□ Administrative root access



Correct

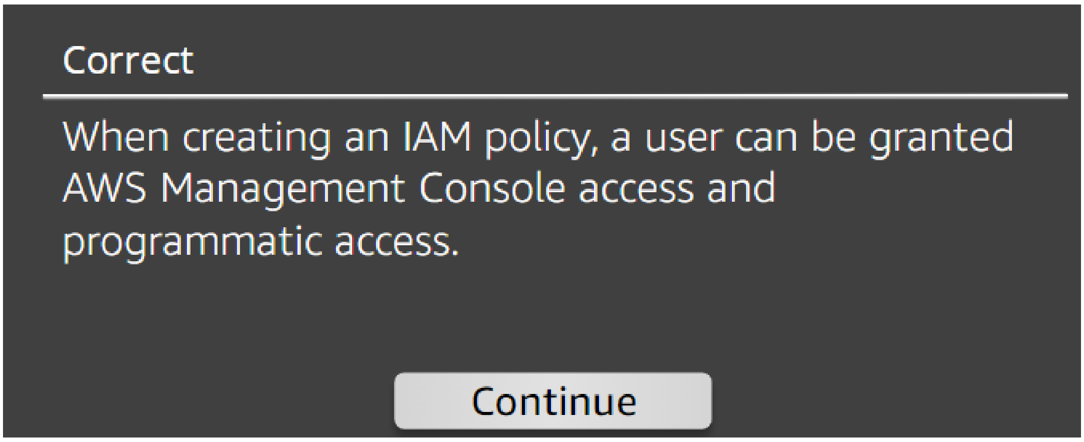
When creating an IAM policy, a user can be granted AWS Management Console access and programmatic access.



5. True or False? AWS Organizations enables you to consolidate multiple AWS accounts so that you centrally manage them.

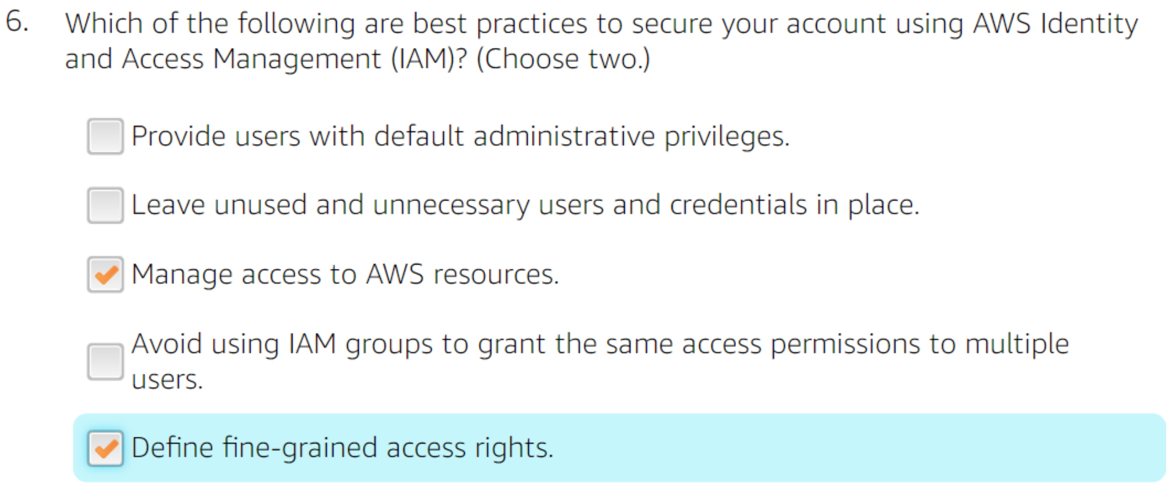
● True

○ False



Correct

When creating an IAM policy, a user can be granted AWS Management Console access and programmatic access.



6. Which of the following are best practices to secure your account using AWS Identity and Access Management (IAM)? (Choose two.)

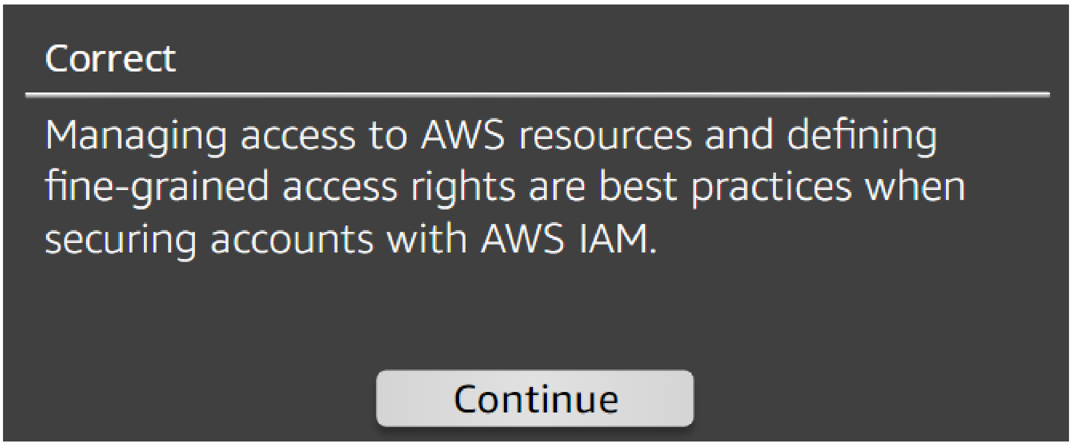
☐ Provide users with default administrative privileges.

☐ Leave unused and unnecessary users and credentials in place.

☑ Manage access to AWS resources.

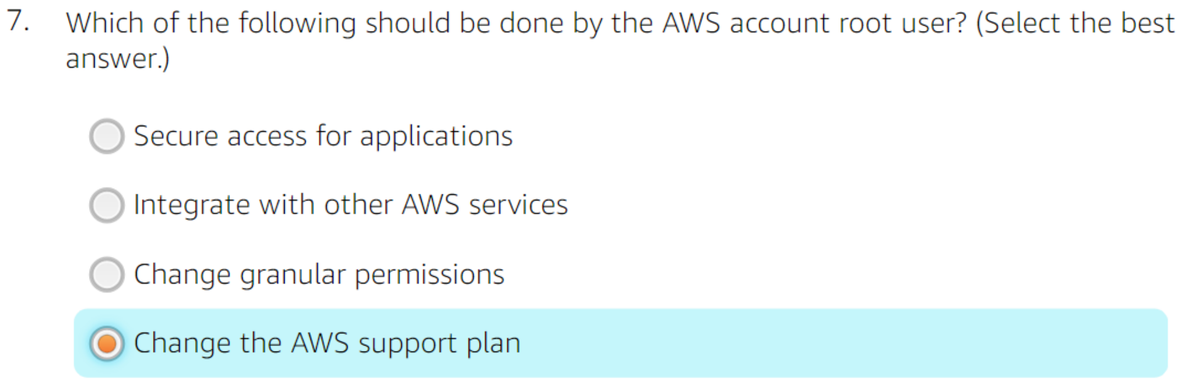
☐ Avoid using IAM groups to grant the same access permissions to multiple users.

☑ Define fine-grained access rights.



Correct

Managing access to AWS resources and defining fine-grained access rights are best practices when securing accounts with AWS IAM.



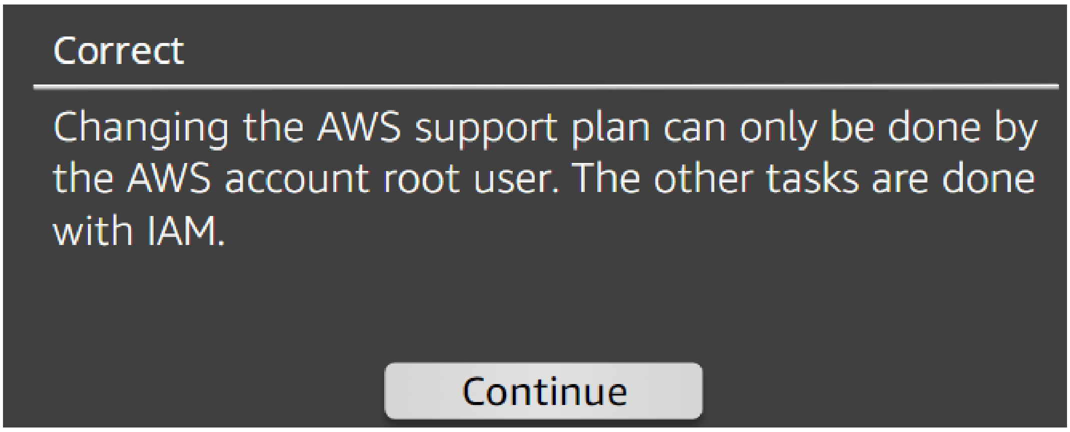
7. Which of the following should be done by the AWS account root user? (Select the best answer.)

○ Secure access for applications

○ Integrate with other AWS services

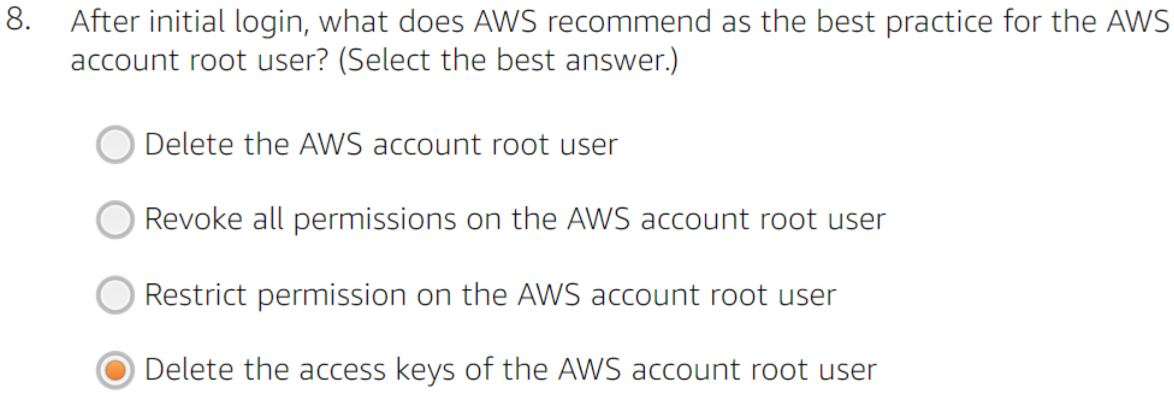
○ Change granular permissions

● Change the AWS support plan



Correct

Changing the AWS support plan can only be done by the AWS account root user. The other tasks are done with IAM.



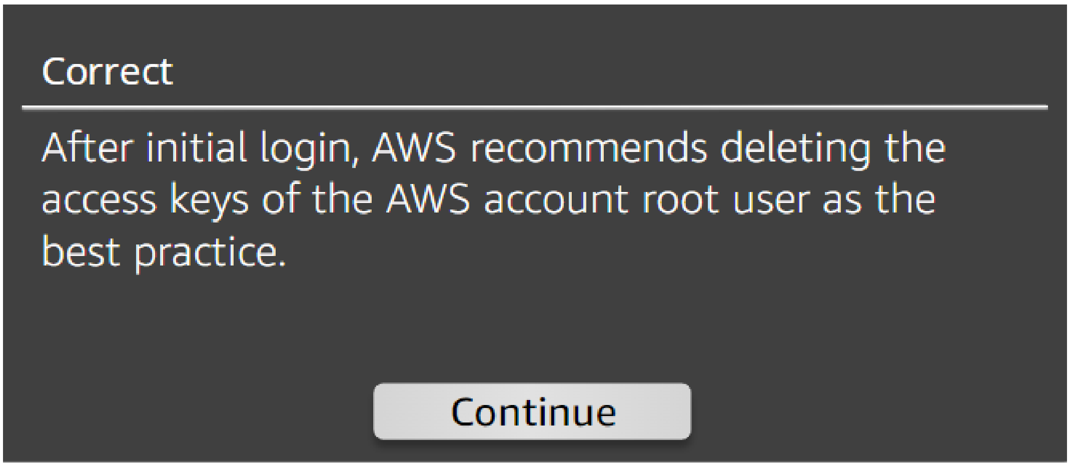
8. After initial login, what does AWS recommend as the best practice for the AWS account root user? (Select the best answer.)

○ Delete the AWS account root user

○ Revoke all permissions on the AWS account root user

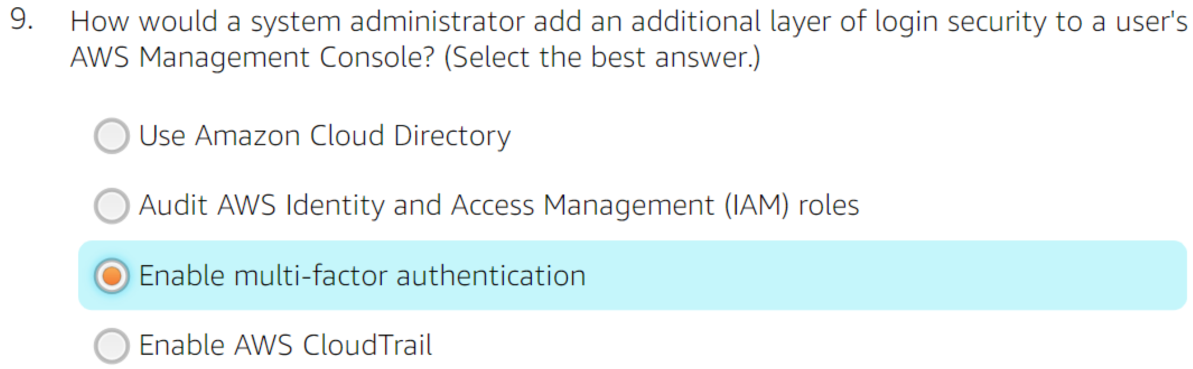
○ Restrict permission on the AWS account root user

● Delete the access keys of the AWS account root user



Correct

After initial login, AWS recommends deleting the access keys of the AWS account root user as the best practice.



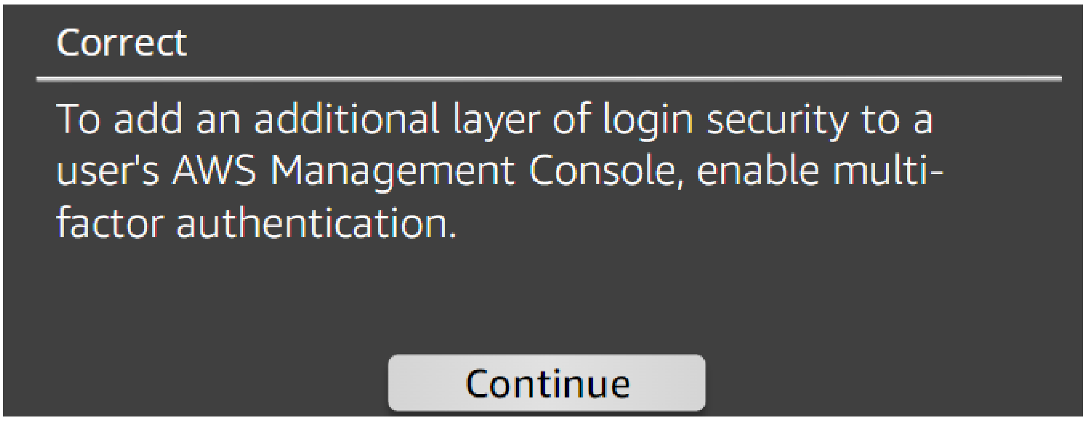
9. How would a system administrator add an additional layer of login security to a user's AWS Management Console? (Select the best answer.)

○ Use Amazon Cloud Directory

○ Audit AWS Identity and Access Management (IAM) roles

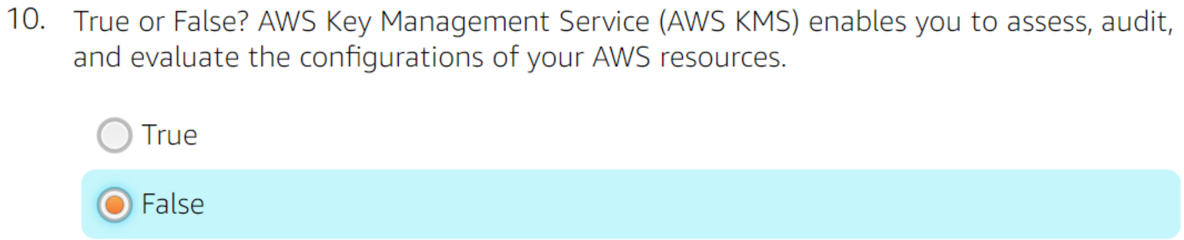
● Enable multi-factor authentication

○ Enable AWS CloudTrail



Correct

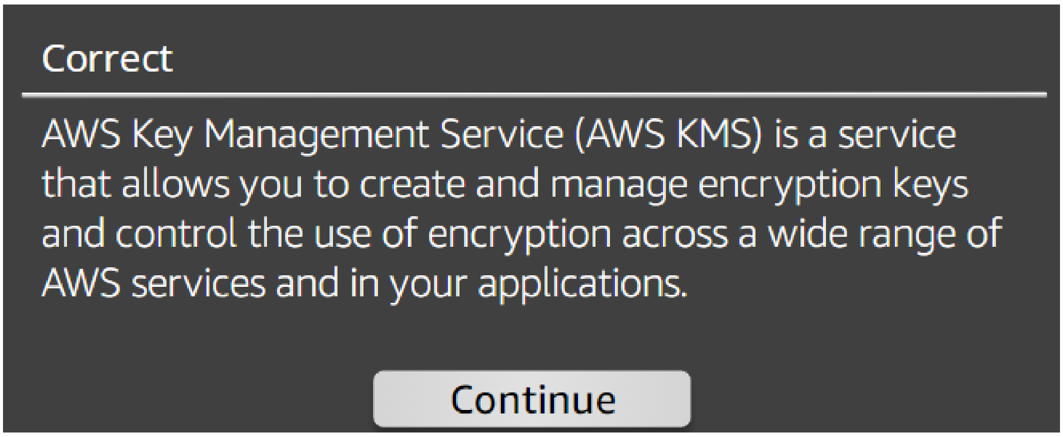
To add an additional layer of login security to a user's AWS Management Console, enable multi-factor authentication.



10. True or False? AWS Key Management Service (AWS KMS) enables you to assess, audit, and evaluate the configurations of your AWS resources.

○ True

● False



Correct

AWS Key Management Service (AWS KMS) is a service that allows you to create and manage encryption keys and control the use of encryption across a wide range of AWS services and in your applications.