

EE4221 Quiz 4

1. In the shared responsibility model, AWS is responsible for providing what?

Security in the cloud	Security to the cloud
Security of the cloud	Security for the cloud

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

Physical security of the facilities in which the services operate
Security group configurations
Compliance with compute security standard and regulations
Protecting the global infrastructure
Encryption of data at rest and data in transit
No Answer

3. Which of the following is the responsibility of AWS under the AS shared responsibility model?

Maintaining physical hardware
Configuring third-party applications
Managing custom Amazon Machine Images (AMIs)
Securing application access and data

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	AWS Management Console access
Administrative root access	Authorised access
Programmatic access	No Answer

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

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

Define fine-grained access rights.
Avoid using IAM groups to grant the same access permissions to multiple users.
Manage access to AWS resources
Leave unused and unnecessary users and credentials in place.
Provide users with default administrative privileges.
No Answer

7. After initial login, what does AWS recommend as the best practice for the AWS account root user?

Delete the AWS account root user
Restrict permission on the AWS account root user
Delete the access keys of the AWS account root user
Revoke all permissions on the AWS account root user
No answer

8. How would a system administrator add an additional layer of login security to a user's AWS Management Console?

Enable AWS CloudTrail
Use Amazon Cloud Directory
Enable multi-factor authentication
Audit AWS Identity and Access Management (IAM) roles
No Answer

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

True	False	No Answer
------	-------	-----------

10. Which of the following could only be done by the AWS account root user?

Secure access for applications	Change granular permissions
Integrate with other AWS services	Change the AWS support plan
No Answer	