Practice Questions, Week 4

1. Which of the following is true about the AWS shared responsibility model? (Select THREE.)

    a) AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates
    b) While AWS manages security of the cloud, security in the cloud is the responsibility of the customer.
    c) The customer may rely on AWS to manage the security of their workloads deployed on AWS.
    d) The customer must audit the AWS data centers personally to confirm the compliance of AWS systems and services.
    e) The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall.

2. Who is responsible for the configuration of security groups in an AWS environment?

    a) The customer and AWS are both jointly responsible for ensuring that security groups are correctly and securely configured.
    b) AWS is responsible for ensuring that all security groups are correctly and securely configured. Customers do not need to worry about security groups configuration.
    c) AWS provides the security groups functionality as a service, but the customer is responsible for correctly and securely configuring their own security groups.
    d) Neither AWS nor the customer is responsible for the configuration of security groups; security groups are intelligently and automatically configured using traffic heuristics.

3. Which of the following Amazon Virtual Private Cloud (Amazon VPC) elements acts as a stateless firewall?

    a) Security group
    b) Network Access Control List (NACL)
    c) Network Address Translation (NAT) instance
    d) Amazon VPC endpoint

4. Which of the following statements is true when it comes to the risk and compliance advantages of the AWS environment?

    a) Workloads must be moved entirely into the AWS Cloud in order to be compliant with various certifications and third-party attestations.
    b) The critical components of a workload must be moved entirely into the AWS Cloud in order to be compliant with various certifications and third-party attestations, but the non-critical components do not.
    c) Few, many, or all components of a workload can be moved to the AWS Cloud, but it is the customer's responsibility to ensure that their entire workload remains compliant with various certifications and third-party attestations.
    d) The non-critical components of a workload must be moved entirely into the AWS Cloud in order to be compliant with various certifications and third-party attestations, but the critical components do not.

5. You are designing an application within AWS that requires PCI Compliance. You would therefore like access to security and compliance reports for the underlying AWS systems. Which service can you use to access this documentation?

    a) AWS Artifact
    b) AWS CloudTrail
    c) AWS CodeBuild
    d) Raise a support request, AWS staff will then provide access to the documents using Amazon S3

6. You have an application that will run on an Amazon EC2 instance. The application will make requests to Amazon S3 and Amazon DynamoDB. Using best practices, what type of AWS Identity and Access Management (IAM) principal should you create for your application to access the identified services?

    a) IAM user
    b) IAM group
    c) IAM role
    d) IAM directory

7. Your security team is very concerned about the vulnerability of the IAM administrator user accounts. What steps can be taken to lock down these accounts? (Select THREE.)

    a) Implement a password policy on the AWS account
    b) Limit logins to a particular U.S. state
    c) Add multi-factor authentication (MFA) to the accounts
    d) Apply a source IP address condition to the policy that only grants permissions when the user is on the corporate network
    e) Add a CAPTCHA test to the accounts

8. Which AWS service automatically conducts security assessments of your applications deployed on AWS and provides you with a detailed list of security findings prioritized by level of severity?

    a) AWS Systems Manager
    b) Amazon CloudWatch
    c) Amazon Macie
    d) Amazon Inspector

9. Your company has been a victim of a Distributed Denial-of-Service (DDoS) attack in the past. You want to prevent another DDoS attack by ensuring that you can distribute your users (including illegitimate requests) across multiple regions. Which AWS service will help you achieve this?

    a) AWS WAF
    b) Amazon CloudFront
    c) AWS Shield
    d) Auto Scaling

10. Which AWS service records API calls made on your account and delivers log files to your Amazon S3 bucket?

    a) Amazon CloudWatch
    b) Amazon Kinesis
    c) AWS Data Pipeline
    d) AWS CloudTrail

Answers

1) a, b, e; 2) c; 3) b; 4) c; 5) a; 6) c; 7) a, c, d; 8) d; 9) b; 10) d