Cloud Computing (CS4075)

Sessional-I Exam

Course Instructor(s):
Mr Zaheer Sani
Section(s): BSSE-A

Total Time (Hrs): 1
Total Marks: 45
Total Questions: 3

Date: Sep 23, 2024

Roll No 21-0515

Course Section SE-A

Student Signature

Attempt all the questions.

Question 1 [0.5 x 30 = 15 Marks]

Instructions: Fill the attached bubble sheet. Marks will not be given if sheet is not filled properly.

1. Which of the following methods is not a valid way to interact with AWS services?

A) AWS CLI	B) AWS SDKs	C) AWS Management Console	D) RESTful APIs	E) All of the them

2. DynamoDB is associated with which type of database system?

A) Relational (SQL) database	B) Non-relational (NoSQL) database	C) Elastic File Storage	D) Serverless computing	E) Elastic computing

3. Which of the following is not an advantage of cloud computing compared to on-premises infrastructure?

A) On-demand scalability	B) Global deployment in minutes	C) Faster innovation and agility	D) Eliminating the need for upfront hardware investments	E) None of the above

4. What pricing model allows AWS customers to only pay for the resources they actually use?

A. Pay as you need	B. Pay as you go	C. Pay as you buy	D. Pay as you reserve	E) AURI

5. Which of these is NOT a cloud computing model?

A) Platform as a service	B) Infrastructure as a service	C) Cloud provider as a service	D) Software as a service

6. What is meant by "economies of scale" in the context of cloud computing?

A) Building large clusters or clouds using low-cost hardware	B) Increasing speed as user demand grows	C) Cloud providers having more financial scalability	D) A larger user base leads to lower service costs	E) Dynamic scaling of users with pay-as-you-go

7. Which of the following is not a cloud computing benefit compared to on-premises infrastructure?

A) Increased speed and agility	B) Capital investment for resources	C) Eliminating the need to guess infrastructure capacity	D) Replacing capital expenses with variable expenses	E) Gaining from economies of scale

8. Which of the following is an AWS compute service?

A) S3	B) EC2	C) CloudFront	D) VPC	E) IAM

9. Which AWS service represents AWS Content Delivery Network (CDN) implementation?

A) Availability Zones	B) Route 53	C) CloudFront	D) VPC	E) IAM

10. For services like Amazon EC2 and Amazon RDS, which of the following is not a valid reserved instance option?

| A) AURI | B) MURI | C) NURI | D) PURI |

11. Where can a customer go to get more details about Amazon EC2 billing activity from 3 months ago?

| A) Amazon EC2 dashboard | B) AWS Trusted Advisor dashboard | C) AWS Cost Explorer | D) AWS CloudTrail logs |

12. To receive the discounted rate associated with Reserved Instances, must you make a full upfront payment for the entire term of the agreement?

| A) True | B) False |

13. Which statement is true regarding AWS pricing models?

| A) Per gigabyte charge for inbound data transfer | B) Storage is typically charged per gigabyte | C) Compute is typically charged as a monthly fee based on instance type | D) Outbound charges are free up to a per account limit |

14. What are the four support plans offered by AWS Support?

| A) Basic, Developer, Business, Enterprise | B) Basic, Startup, Business, Enterprise | C) Free, Bronze, Silver, Gold | D) AWS Free Tier | E) All of the above |

15. Which AWS tool allows you to explore services and create an estimate for your business use case costs?

| A) AWS Pricing Calculator | B) AWS Budgets | C) AWS Cost and Usage Report | D) AWS Billing Dashboard | E) Economies of scale |

16. Why might local laws restrict the choice of AWS Regions for hosting content or services?

| A) To promote AWS services | B) To encourage cross-region data replication | C) To reduce latency for users | D) To ensure data governance and compliance with legal requirements |

17. What is one key advantage of hosting applications and data in a Region close to the users?

| A) Reduced latency | B) Reduced cost of hosting | C) Reduced data replication requirements | D) Enhanced security |

18. Why might local laws restrict the choice of AWS Regions for hosting content or services?

| A) To promote AWS services | B) To encourage cross-region data replication | C) To reduce latency for users | D) To ensure data governance and compliance with legal requirements |

19. What is one key advantage of hosting applications and data in a Region close to the users?

| A) Reduced latency | B) Reduced cost of hosting | C) Reduced data replication requirements | D) Enhanced security |

20. Why is it important to verify AWS service availability in a specific Region before deploying?

| A) All AWS services are available in all Regions. | B) Different Regions have different pricing for the same services. | C) Some AWS services may not be available in all Regions. | D) Availability of services does not vary by Region. |

21. What is the primary purpose of Availability Zones within an AWS Region?

| A) Isolation from other AWS Regions | B) Low-latency networking | C) Cost-effective data storage | D) High availability, fault tolerance, and scalability |

22. How many data centers are typically included in each Availability Zone?

| A) One to Three | B) ten to fifteen | C) Hundreds | D) fifty to sixty |

23. How are Availability Zones physically isolated from one another?

| A) They are located in different AWS Regions. | B) They share power infrastructure. | C) They use shared fiber-optic cables. | D) They are physically separated by many kilometers. |

24. Who is responsible for choosing the Availability Zones for AWS deployments?

| A) AWS support engineers | B) AWS administrators | C) AWS customers | D) AWS availability experts |

25. What is the primary role of Amazon CloudFront and Amazon Route 53 in the AWS infrastructure?

A) To reduce latency for end users	B) To provide compute resources	C) To manage AWS billing	D) To deliver content to edge locations

26. What is the primary advantage of using AWS Lambda?

A) It provides resizable compute capacity.	B) It supports Docker containers.	C) You pay only for compute time consumed.	D) It automatically manages block storage.

27. Which deployment model allows organizations to integrate their existing infrastructure with cloud services while connecting cloud resources to internal systems?

A) Cloud	B) On-Premises	C) Multi-Cloud	D) Hybrid

28. When data is stored in a specific AWS Region, what happens to that data?

A) It is automatically replicated to other Regions.	B) It is replicated to a secondary data center within the same Region.	C) It is not replicated outside that Region.	D) It is replicated to all other AWS Regions by default.

29. How can you enable or disable an AWS Region for use in your account?

A) By contacting AWS customer support	B) By purchasing a special AWS Region access plan	C) By using the AWS Management Console	D) By modifying the AWS Region configuration file

30. What are IAM users in AWS?

A) Virtual machines used to manage AWS resources	B) Identities that represent individual people or services with access to AWS resources	C) Applications that manage AWS resources automatically	D) Resources that can be attached to AWS instances

Question 2 [10 x 2 = 20 Marks]

Consider the following scenarios and choose the most appropriate option. You also need to provide the justification for your answer in 2-3 lines.

1. Scenario: Your company has several developers working on different AWS projects. Each developer needs access to specific services such as EC2 and S3, but not all of them require full administrative access to AWS resources. You want to manage these permissions efficiently.

Question: How would you structure your IAM permissions to ensure that developers have only the necessary access to the AWS resources they need while following best practices for security?

A) Assign administrative permissions to all developers to avoid any permission issues.
B) Create individual IAM users for each developer and attach the necessary permissions directly to their user accounts.
C) Create IAM groups with specific permissions (e.g., one for EC2 access, one for S3 access) and assign developers to the appropriate groups.
D) Use the root user to manage developer access to ensure control over all resources.

2. Scenario: You are building a web application that will run on Amazon EC2 instances. The application needs to upload files to an S3 bucket. You want to avoid hardcoding AWS credentials within your application.

Question: What is the best way to grant your EC2 instances the necessary permissions to upload files to the S3 bucket?

A) Create an IAM user with access to S3 and store the credentials on the EC2 instances.
B) Attach an IAM role with S3 write permissions to the EC2 instances so they can assume the role when accessing the bucket.
C) Enable the EC2 instances to access AWS resources without credentials.
D) Hardcode the IAM user credentials in the application code to access the S3 bucket.

3. Scenario: Your organization has several third-party contractors who need temporary access to your AWS resources for a specific project. You want to ensure they have limited access and that their permissions automatically expire after the project is completed.

Question: What is the best approach to provide secure and temporary access to these contractors?

A) Create individual IAM users for each contractor and delete the accounts after the project.
B) Create an IAM role with the necessary permissions and allow the contractors to assume the role for a limited duration using temporary credentials.
C) Share the root account credentials with the contractors and change the password after the project ends.
D) Create IAM policies that block all permissions after a specific date and apply them to the contractors.

4. Scenario: Your team is working on a new project where some team members only need read-only access to certain S3 buckets, while others need full access. You want to make it easy to manage these permissions as the team grows.

Question: How would you implement IAM policies to manage these access levels effectively?

A) Create a single IAM policy with full access and apply it to all team members.
B) Create two separate IAM policies—one for read-only access and another for full access—and assign them to different IAM groups for the team.
C) Attach individual permissions directly to each team member's IAM user based on their role.
D) Use the root user to manage access for the team.

5. Scenario: You notice suspicious activity in your AWS account and suspect that one of your IAM users' credentials has been compromised. You need to respond quickly to secure your AWS resources.

Question: What steps should you take to mitigate this situation and prevent further unauthorized access?

A) Immediately delete the compromised IAM user and all associated resources.
B) Revoke the compromised IAM user's access keys and passwords, and rotate them.
C) Disable the root user account and monitor AWS CloudTrail logs for unusual activity.
D) Use AWS Trusted Advisor to check for any service disruptions caused by the compromised user.

6. Scenario: Your organization uses IAM policies to control access to S3 buckets. You want to ensure that only certain IAM users can delete objects from the buckets, while others can only view the content.

Question: How would you structure your IAM policy to meet this requirement?

A) Use a single policy that allows all users full access to the S3 bucket.
B) Create two separate policies: one that grants delete permissions and another that only grants read permissions, and apply them to the respective IAM users or groups.
C) Apply full access to the root user and delegate read-only permissions to all other users.
D) Create a policy that denies delete actions for all users except the root user.

7. Scenario: You are responsible for securing your company's AWS environment, and you want to ensure that only IAM users with MFA enabled can access sensitive resources such as EC2 and RDS instances.

Question: How can you enforce this security policy using IAM?

A) Create an IAM role that automatically enables MFA for all users accessing EC2 and RDS.
B) Set up a service control policy (SCP) to block access to EC2 and RDS unless MFA is enabled.
C) Apply an IAM policy that requires MFA for accessing EC2 and RDS resources and assign it to the relevant IAM users or groups.
D) Disable access to EC2 and RDS until MFA is set up for all users.

National University of Computer and Emerging Sciences
Islamabad Campus

8. Scenario: A new compliance requirement mandates that all API calls made to AWS resources must be logged. You want to ensure that any actions performed by IAM roles are tracked for auditing purposes.

Question: What service should you use to log and track API calls made by IAM roles?

A) AWS CloudWatch B) AWS CloudTrail C) AWS Trusted Advisor D) AWS Shield

9. Scenario: You need to provide temporary, limited access to a partner organization to read data from one of your S3 buckets. However, you don't want to create an IAM user for them.

Question: What is the most secure way to provide this access?

A) Share your root account credentials with the partner
B) Create an IAM role with S3 read access and allow the partner to assume the role using temporary credentials
C) Create a public bucket policy and share the URL with the partner
D) Provide them with an IAM user's access key and secret key for direct access.

10. Scenario: You have multiple AWS accounts and want to allow users in one account to access resources in another account using IAM roles.

Question: How would you configure IAM roles to allow cross-account access?

A) Create a new IAM user in each account with the necessary permissions.
B) Create a role in the target account and define a trust relationship that allows users from the source account to assume that role.
C) Share IAM user credentials between accounts.
D) Enable cross-account access by default for all users in both accounts.

Question 3 [10 Marks]

You are tasked with designing architecture for a new web application on AWS. The application will have the following requirements:

- **User authentication** should be handled by AWS scalable managed solution.
- **Application compute power** will be needed to handle dynamic requests.
- **Data storage** for user-uploaded files, such as images and documents.
- **Relational database** for managing user data and transactions with auto-backup and patching feature.
- **Access control** to ensure that only authorized services and users can interact with AWS resources.

Draw an architecture diagram which represents and connects the services required in above scenario.