

[Part-A]

Choose the correct Options and Mark on Bubble Sheet only. [30 marks]

1. Your organization has multiple accounts in AWS Organizations, and you need to monitor and audit activities across all accounts. Which service allows you to centralize logging and auditing of API calls in all AWS accounts within your organization?
 - a. AWS CloudWatch
 - b. AWS Config
 - c. AWS CloudTrail
 - d. AWS Security Hub
 - e. AWS CloudFront
2. Which of the following AWS services is a NoSQL database?
 - a. Amazon RDS
 - b. Amazon DynamoDB
 - c. Amazon Aurora
 - d. Amazon Redshift
 - e. Amazon S3
3. What is Amazon S3 used for?
 - a. Compute service
 - b. Object storage
 - c. Database management
 - d. Networking
 - e. Virtual machines
4. Which AWS service allows you to create and manage virtual networks?
 - a. Amazon VPC
 - b. AWS Lambda
 - c. AWS Direct Connect
 - d. Amazon EC2
 - e. Amazon S3
5. Which AWS service provides content delivery?
 - a. Amazon VPC
 - b. Amazon Route 53
 - c. AWS CloudFront
 - d. AWS Direct Connect
 - e. Amazon S3
6. What is AWS Elastic Beanstalk used for?
 - a. Serverless architecture

- 12
National
- b. Container orchestration
 - c. Automatic scaling of resources
 - d. Hosting web applications
 - e. Object storage
7. What does AWS Lambda charge you for?
- a. Number of requests and duration of execution
 - b. Number of resources used
 - c. Storage size
 - d. Compute capacity
 - e. Network traffic
8. What is the main use of Amazon CloudTrail?
- a. To monitor logs and events in your AWS environment
 - b. To manage network traffic
 - c. To encrypt data
 - d. To set up firewall rules
 - e. To deploy applications
9. Which AWS service is primarily used for managing Cryptographic Keys?
- a. Amazon ECS
 - b. Amazon EKS
 - c. Amazon KMS
 - d. AWS shield
 - e. Amazon Secrets Manager
10. What is a subnet mask used for?
- a. To divide an IP address into network and host portions
 - b. To provide security on a network
 - c. To assign IP addresses dynamically
 - d. To encrypt network traffic
 - e. To route data between networks
11. You are running a high-traffic e-commerce website hosted on EC2 instances. To ensure that your website can handle traffic spikes during peak shopping seasons, what AWS service should you use to automatically adjust the number of EC2 instances based on demand?
- a. Amazon Elastic Load Balancer
 - b. Amazon CloudWatch
 - c. Amazon EC2 Auto Scaling
 - d. Amazon VPC
 - e. Amazon RDS

12. Your application relies on a relational database and you need to ensure high availability with automated failover to a secondary instance. What is the best solution for this scenario on AWS?
 - a. Amazon RDS Multi-AZ Deployment
 - b. Amazon EC2 with manual backups
 - c. Amazon ElastiCache
 - d. AWS Lambda with a NoSQL database
 - e. Amazon S3
13. You need to configure your AWS architecture for disaster recovery with minimal downtime. Which of the following strategies would you choose for your EC2 instances?
 - a. Backup EC2 instances and restore from Amazon S3 in case of failure
 - b. Use AWS Elastic Load Balancer to distribute traffic across multiple regions
 - c. Set up EC2 instances in multiple Availability Zones with Auto Scaling
 - d. Use EC2 Spot instances to reduce costs
 - e. Store all logs in Amazon S3
14. You have a web application hosted in an Amazon VPC and you want to allow users to access it securely from the internet. What should you do to ensure secure, controlled access to your VPC resources?
 - a. Configure a public subnet with a security group
 - b. Create a VPN connection to an on-premises data center
 - c. Set up an Internet Gateway and route traffic to the public subnet
 - d. Use AWS Direct Connect for dedicated network connectivity
 - e. Use an Elastic Load Balancer with SSL termination
15. Your team is managing sensitive data, and you need to ensure that it is encrypted both in transit and at rest. Which AWS services and configurations would meet this requirement?
 - a. Use AWS Lambda and encrypt the data with KMS before storing in Amazon S3
 - b. Use Amazon EC2 with VPN connections and encrypt data using SSL
 - c. Use Amazon RDS with Multi-AZ and enable encryption at rest
 - d. Use Amazon S3 with server-side encryption and HTTPS for data transmission
 - e. All of the above
16. You are running a global application and want to ensure low-latency access for users in different regions. Which AWS service should you use to distribute content to users with minimal delay?
 - a. Amazon Route 53
 - b. AWS Global Accelerator
 - c. Amazon CloudFront
 - d. Amazon S3
 - e. AWS Direct Connect

National University of Computer and Emerging Sciences
Islamabad Campus

17. You need to deploy a web application but don't want to manage the underlying server, operating systems, or databases. Which cloud service model should you choose?
- a. Infrastructure as a Service (IaaS)
 - b. Platform as a Service (PaaS)
 - c. Software as a Service (SaaS)
 - d. Data as a Service (DaaS)
 - e. Cloud Storage as a Service
18. Which of the following is a disadvantage of cloud computing?
- a. Lower costs due to on-demand pricing
 - b. Increased flexibility and scalability
 - c. Potential data security and privacy concerns
 - d. Ease of integration with on-premises infrastructure
 - e. High availability and uptime
19. Which of the following disadvantages of cloud computing could affect users during a service outage?
- a. Guaranteed data privacy and security
 - b. Reduced risk of data loss
 - c. No access to services or data during downtime
 - d. Automatic scalability
 - e. Reduced flexibility in pricing
20. Your company has a predictable workload and requires EC2 instances for a long period, with minimal changes to usage over time. Which AWS pricing option would be most cost-effective in this case?
- a. On-Demand Instances
 - b. Reserved Instances
 - c. Spot Instances
 - d. Savings Plans
 - e. Dedicated Hosts
21. Your organization wants to restrict the usage of certain services in specific accounts in your AWS Organization. Which feature allows you to enforce restrictions on what actions can be performed at the account level?
- a. AWS Identity and Access Management (IAM) Policies
 - b. AWS Organizations Service Control Policies (SCPs)
 - c. AWS CloudTrail Logs
 - d. AWS Config Rules
 - e. AWS Shield
22. Which of the following is a key component of AWS's global infrastructure that is used to distribute AWS services globally?
- a. Regions

- b. Availability Zones
 - c. Edge Locations
 - d. Data Centers
 - e. All of the above
23. What is the main purpose of having multiple Availability Zones (AZs) in a Region?
- a. To provide low-latency access to AWS services
 - b. To increase the availability and fault tolerance of AWS services
 - c. To reduce the cost of running services on AWS
 - d. To offer high-speed networking between regions
 - e. To manage customer access to AWS resources globally
24. You are the administrator for your company's AWS account. Your team uses IAM roles to manage access to resources. A user has reported being unable to access an S3 bucket they need for their work, even though they are assigned to a role that has permissions for this S3 bucket. Upon investigation, you find that the IAM role has the necessary permissions, but the user still cannot access the bucket. What is the most likely cause?
- a. The user's IAM policy is conflicting with the role's permissions.
 - b. The user is in a different AWS Region than the S3 bucket.
 - c. There is a Service Control Policy (SCP) applied in AWS Organizations preventing access.
 - d. The S3 bucket has a bucket policy that denies access from the user's account.
 - e. The IAM role does not have the correct trust relationship policy.
25. A user in your AWS account has reported issues accessing an S3 bucket that they need for their daily tasks. You checked the IAM policy attached to the user, and it looks correct. You also verified the S3 bucket policy, and everything seems in order. What is the next step to troubleshoot this issue?
- a. Check the AWS CloudTrail logs for denied actions related to the user.
 - b. Verify the IAM user's password policy.
 - c. Reset the IAM user's access keys.
 - d. Review the CloudWatch logs for the S3 bucket.
 - e. Check the EC2 instance's security group rules.
26. You are tasked with enforcing the use of MFA for all IAM users in your organization when accessing AWS resources. You also want to ensure that IAM users without MFA enabled cannot make any API calls to AWS services. What would be the best approach to enforce this policy?
- a. Attach an MFA-required policy to each user manually.
 - b. Modify the IAM group policy to deny access if MFA is not enabled.
 - c. Use an IAM policy that explicitly denies all actions unless MFA is enabled.
 - d. Enable MFA through AWS Organizations and enforce it for all accounts.
 - e. Use AWS Identity Federation to enforce MFA.

National University of Computer and Emerging Sciences
Islamabad Campus

Nation

Note: User

27. Your company is setting up a new IAM policy for the "Admin" group, which requires full access to all AWS resources. After assigning the policy, you notice that an IAM user in the "Admin" group is unable to perform some administrative actions. What could be the cause of this issue?
- a. The user is missing the iam:CreatePolicy permission.
 - b. The IAM group policy explicitly denies certain administrative actions.
 - c. The IAM user is assigned a conflicting deny policy from another group.
 - d. IAM groups cannot grant permissions beyond those already granted to individual users.
 - e. The IAM group policy needs to be assigned at the region level to take effect.
28. You are tasked with securing sensitive data stored in Amazon RDS. Which of the following options will ensure that data is encrypted both in transit and at rest?
- a. Use SSL/TLS encryption for connections to RDS, and enable encryption at rest using KMS-managed keys.
 - b. Enable automatic backups to secure the data at rest.
 - c. Encrypt data in transit using an HTTPS connection, and disable encryption at rest for performance.
 - d. Use IAM policies to enforce encryption for all RDS instances.
 - e. Enable security groups to restrict access, and configure data replication for security.
29. Your organization uses Amazon CloudTrail to monitor all API activity within your AWS account. However, you want to ensure that CloudTrail logs are encrypted and only accessible by certain administrators. What should you do to meet this requirement?
- a. Configure CloudTrail to store logs in an S3 bucket and enable server-side encryption with AWS KMS.
 - b. Use IAM policies to restrict access to CloudTrail logs based on the user's role.
 - c. Enable CloudTrail logs to be delivered only to an encrypted EBS volume.
 - d. Enable AWS Shield protection for CloudTrail logs to secure them from unauthorized access.
 - e. Store CloudTrail logs in an encrypted DynamoDB table with fine-grained access control.
30. You are building an application where users can upload photos and videos. These media files should be stored in the cloud, and you want to ensure the storage is highly durable, cost-effective, and easy to manage. Additionally, the files need to be publicly accessible for sharing via URLs. Which AWS service should you use to store the media files?
- a. Amazon EFS
 - b. Amazon S3
 - c. Amazon Glacier
 - d. Amazon EBS
 - e. Amazon RDS

[Part-B]

Note: Use Answer sheet for this part.

Scenario:

You are a cloud administrator for a small e-commerce startup that is using AWS for hosting their web applications and databases. The startup is growing and experiencing an increase in customer visits, so the management wants to ensure their infrastructure is secure, scalable, and cost-effective.

Your job is to design a solution that addresses the following needs:

Requirements:

i. **Security:**

- a. You need to ensure that sensitive customer data, such as payment information, is stored securely and can only be accessed by authorized users.
- b. You should implement a method to manage access to AWS resources and ensure that users only have the permissions they need.

ii. **Scalability:**

- a. The startup expects fluctuating traffic and wants to scale their infrastructure automatically based on demand, particularly during sales events.

iii. **Cost Optimization:**

- a. The company wants to minimize AWS costs, especially as it grows, but still maintain the ability to scale during peak times.

Q2: Design a secure solution to store sensitive customer data such as payment information and ensure that only authorized employees can access it. Mention any two strategies. **[4+4 Marks]**

Q3: Design an auto-scaling solution to handle fluctuating web traffic during sales and ensure that resources are only utilized as needed during off-peak times. Mention any two strategies. **[4+4 Marks]**

Q4: Implement a cost-effective infrastructure, ensuring that the startup can scale as needed but avoid paying for unused resources during non-peak hours. Mention any two strategies. **[4+4 Marks]**