AWS TEST

1. If your application requires large amounts of memory for high-performance databases or in-memory analytics, which instance type is most suitable?

A) Compute Optimized Instances (C instances)

B) General Purpose Instances (M instances)

C) Memory Optimized Instances (R or X instances)

D) Accelerated Computing Instances (P instances)

2. How does Amazon EC2 Auto Scaling respond during a sudden increase in traffic?

A) Automatically increases the number of instances based on defined policies

B) Terminates all existing instances and creates new ones

C) Sends an alert without changing the number of instances

D) Reduces the number of instances to conserve resources

3. What is a common way to configure Amazon EC2 Auto Scaling to handle periods of high and low traffic automatically?

A) Use Scheduled Scaling to increase instances during peak hours and reduce during off-hours

B) Manually start and stop instances based on estimated traffic

C) Set up only the minimum instance count

D) Disable the Auto Scaling Group during low traffic

4. What is a key purpose of a multi-tier architecture on Amazon EC2?

A) To increase the storage capacity of EC2 instances

B) To separate different layers of an application for better performance, scalability, and security

C) To enable automatic backup of all application data

D) To reduce the cost of deploying applications on AWS

5. Which of the following is NOT a typical component included in an Amazon Machine Image (AMI)?

A) Operating system

B) Application software

C) Networking configuration for a VPC

D) Application server configuration

6. What is a primary difference between Dedicated Hosts and Dedicated Instances?

A) Only Dedicated Instances allow customers to bring their own licenses (BYOL)

B) Only Dedicated Hosts provide control over physical host-level configurations

C) Dedicated Instances provide control over hardware but not billing

D) Dedicated Hosts are automatically assigned to multiple users

7. How does Elastic Load Balancing improve the fault tolerance of an application hosted on Amazon EC2?

A) By automatically scaling EC2 instances during traffic spikes

B) By distributing traffic across multiple instances, reducing the impact of a single instance failure

C) By creating backups of EC2 instances

D) By reducing the storage needs of the application

8. When should you consider using a Network Load Balancer over an Application Load Balancer?

A) When low latency and high throughput are required for TCP traffic

B) When you need to route traffic based on HTTP headers

C) When you require SSL termination at the load balancer

D) When you are only serving static content

9. What is the primary purpose of encrypting Amazon EBS volumes and snapshots?

A) To increase the I/O performance of the volume

B) To enhance the security of data at rest by protecting it from unauthorized access

C) To lower the cost of storage

D) To ensure the availability of the EBS volume

10. How does Amazon S3 differ from Amazon EBS (Elastic Block Store)?

A) S3 is used for storing persistent block-level data, whereas EBS is used for storing objects

B) S3 is a scalable object storage service, while EBS is a block storage service primarily used for EC2 instances

C) EBS provides highly durable data storage, while S3 does not

D) EBS can store any type of data, while S3 only stores image

11. Which of the following is a key feature of Amazon S3?

A) Provides a file system interface for storage management

B) Can only be used for storage of small files

C) Supports automatic scaling to handle large amounts of data

D) Offers low-latency access for transactional data

12. What is the primary difference between Amazon S3 and Amazon Glacier?

A) Amazon S3 is designed for real-time data access, while Amazon Glacier is designed for long-term, archival storage with retrieval delays

B) Amazon S3 is cheaper than Glacier

C) Glacier is a more scalable solution than S3

D) Glacier supports real-time access, while S3 is intended for batch processing

13. What is the primary use case for Amazon Elastic File System (EFS) compared to S3?

A) EFS is designed for scalable object storage, while S3 is designed for file storage

B) EFS provides a scalable file storage system for shared access among EC2 instances, while S3 is an object storage service

C) EFS is ideal for data backups, while S3 is better for web content storage

D) EFS is a cheaper alternative to S3 for all use cases

14. Which of the following features does Amazon S3 support to manage access control to stored objects?

A) User Access Control Lists (ACLs) and bucket policies

B) EC2 Instance Policies

C) IAM roles only

D) Access is granted based on the instance type

15. What is the key difference between IAM users and IAM roles?

A) IAM users are associated with temporary credentials, while IAM roles are associated with permanent credentials

B) IAM users are used to grant permissions to AWS resources, while IAM roles cannot be used for permissions

C) IAM roles provide temporary credentials for AWS services or users, while IAM users have permanent credentials

D) IAM roles cannot be used for AWS services, while IAM users can

16. Which of the following is a correct use case for an IAM role?

A) Giving a user access to an EC2 instance for long-term management

B) Allowing an application on an EC2 instance to access other AWS resources temporarily

C) Granting a user permanent administrative access to an S3 bucket

D) Creating a backup of user credentials

17. How can you make a policy more secure by restricting access to specific resources?

A) By using the Resource element in the policy

B) By using the Action element in the policy

C) By using only the Effect element

D) By using only the Condition element

18. What does the Effect element in an IAM policy specify?

A) The specific user to which the policy applies

B) Whether the action is allowed or denied

C) The condition for the policy

D) The region where the policy is valid

19. When configuring route tables for a VPC, what is the significance of the "destination" field?

A) It defines the allowed protocols for traffic

B) It specifies the target for the traffic, such as an IP address or gateway

C) It determines the type of instances that can access the route

D) It specifies which services are available in the VPC

20. Which of the following is true about the main route table in an Amazon VPC?

A) The main route table cannot be modified

B) The main route table is automatically associated with every subnet in the VPC unless another route table is specified

C) The main route table only applies to private subnets

D) It is used only for internet-bound traffic

21. What is the primary difference between a Single-AZ deployment and a Multi-AZ deployment in Amazon RDS?

A) Single-AZ deployment provides higher availability and fault tolerance

B) Multi-AZ deployment replicates data across multiple Availability Zones for high availability

C) Single-AZ deployments only support read replicas

D) Multi-AZ deployments are used only for non-relational databases

22. In Amazon RDS, how does point-in-time recovery work?

A) It restores the database to the most recent backup snapshot only

B) It allows you to recover the database to any specific second within the backup retention period

C) It allows you to restore the database to any day within the backup retention period

D) It uses logs to restore data to the time when the database was first created

23. How can read replicas in Amazon RDS be used for disaster recovery?

A) By storing read replicas across multiple AWS accounts

B) By using read replicas to offload backup storage

C) By promoting a read replica to the primary instance in case of failure of the primary instance

D) By creating periodic snapshots of read replicas

24. How does replication work between the primary instance and the read replica in Amazon RDS?

A) Data is replicated synchronously to ensure zero lag

B) Data is replicated asynchronously to reduce the load on the primary instance

C) Data is replicated using manual snapshots only

D) Data is replicated over VPN tunnels to increase security

25. What is the purpose of CloudWatch Alarms?

A) To collect log data from AWS resources

B) To trigger actions based on metric thresholds, such as sending notifications or auto-scaling

C) To store and archive CloudWatch logs

D) To create customized dashboards for visualizing metrics

26. What is the primary function of CloudWatch Events?

A) To visualize metrics and performance

B) To manage logs and store data

C) To detect and respond to changes in AWS resources and trigger actions

D) To set custom metric thresholds

27. Which of the following is a key feature of AWS CloudTrail?

A) It enables you to view and visualize CloudWatch metrics

B) It allows real-time scaling of AWS resources

C) It provides logs of all API calls made within your AWS account

D) It stores data backups for AWS resources

28. How does CloudTrail improve incident response and troubleshooting?

A) By providing real-time monitoring of AWS service performance

B) By offering detailed logs of AWS API calls, including actions, resources affected, and users involved

C) By automatically scaling EC2 instances

D) By backing up data automatically when failures occur

29. When should you choose AWS Lambda over EC2?

A) When you need to run long-running applications with a fixed server

B) When you need to run event-driven, short-duration tasks with no infrastructure management

C) When you need to run a containerized application with complex configurations

D) When you need full control over the underlying server and operating system

30. What is the advantage of using security groups instead of allowing all traffic (0.0.0.0/0) in your inbound rules?

A.Security groups improve performance.

B.Security groups simplify network management

C Security groups provide granular control over inbound and outbound traffic

D.Security groups offer built-in intrusion detection

31. You have a public-facing web server (EC2 instance A) in a public subnet and a private database server (EC2 instance B) in a private subnet within the same VPC.How would you configure security groups to allow web traffic to reach instance A while ensuring only instance A can access the database on instance B?

A. Create a single security group with inbound rules allowing HTTP traffic on port 80 from 0.0.0.0/0 (any IP) and an outbound rule allowing all traffic to any IP.

B.Create two security groups: - Security group A for instance A: Allow inbound HTTP traffic on port 80 from 0.0.0.0/0 and outbound all traffic. - Security group B for instance B: Allow inbound traffic only from the security group ID of security group A on port 3306 (MySQL) and outbound all traffic.

C.Create two security groups: - Security group A for instance A: Allow inbound HTTP traffic on port 80 from 0.0.0.0/0 and outbound all traffic. - Security group B for instance B: Deny all inbound and outbound traffic.

D Create a single security group with inbound rules allowing HTTP traffic on port 80 from 0.0.0.0/0 and outbound rules allowing all traffic to the security group ID of security group B.

32. You have a critical application with unpredictable load patterns. The question asks about the best approach to maintain consistent application performance using CloudWatch alarms

A. Configure a scaling policy with a fixed scaling increment/decrement of EC2 instances.

B. Implement a CloudWatch alarm with dynamic scaling based on a pre-defined scaling factor.

C. Utilize a target tracking scaling policy that adjusts the number of EC2 instances to maintain a specific application metric (e.g., average response time) within a target range.

D. Manually scale the Auto Scaling group based on real-time monitoring data.

33. You have a production environment with a single Application Load Balancer (ALB) distributing traffic across two Auto Scaling groups in separate Availability Zones (AZ1 and AZ2). Recently, AZ1 experienced an outage.While traffic continued to flow through the healthy instances in AZ2, some users reported slow response times. What is the MOST LIKELY cause of the slow response times?

A. The healthy instances in AZ2 are overloaded due to all traffic being routed there.

B. The ALB is malfunctioning and needs to be restarted.

C. The security groups for the instances are too restrictive.

D. The health checks for the instances are failing due to the outage in AZ1.

34. What best practice should you follow when configuring security groups?

A. Allow all traffic by default and then gradually add restrictive rules.

B. Start with a restrictive baseline and only allow specific, required traffic.

C. Use the same security group for all resourcesin your VPC.

D. Configure security groups to allow SSH access from anywhere for easy management

35. Your application experiences a sudden surge in traffic. How can the ALB in a multi-AZ configuration automatically scale the EC2 instances to handle the increased load?

A. The ALB cannot auto scale EC2 instances; you need to use an Auto Scaling group.

B. Configure scaling policies within the ALB based on metrics like CPU utilization on the instances.

C. Utilize Spot Instances in the target group, which automatically scale based on demand.

D. The ALB automatically provisions new EC2 instances in healthy AZS

36. You want to implement a highly available database cluster behind an ALB in a multi-AZ configuration. What additional considerations are necessary?

A. Configure the database cluster for read replicas in each AZ for fault tolerance.

B. Utilize a Network Load Balancer (NLB) for lower latency database connections.

C. Implement health checks that target the database health endpoint for monitoring.

D. All the above considerations are important.

37. An Auto Scaling group for a file server experiences frequent scaling actions due to short evaluation periods in CloudWatch alarms. How can you optimize scaling behavior while maintaining responsiveness?

A. Increase the evaluation period for both scaling out and scaling in alarms.

B. Decrease the evaluation period for both scaling out and scaling in alarms.

C. Increase the evaluation period for the scaling out alarm and keep the scaling in period short.

D. Decrease the evaluation period for the scaling out alarm and increase the scaling in period.

38. You have an Auto Scaling group for a web application. You want to scale out (add instances) when CPU utilization exceeds 80% for 5 minutes and scale in (remove instances) when CPU utilization falls below 60% for 10 minutes.

A. Create a single CloudWatch alarm with an "Average" statistic, both thresholds, and a scaling policy for each.

B. Create two separate CloudWatch alarms, one for CPU > 80% (Average, 5 minutes) and another for CPU < 60% (Average, 10 minutes). Use separate scaling policies for each alarm.

C. Configure a single CloudWatch alarm with an "Average" statistic and both thresholds. Use a single scaling policy with a cooldown period.

D. You cannot achieve this with CloudWatch Alarms and Auto Scaling.

39. Your Application Load Balancer (ALB) is experiencing a sudden increase in traffic. What is the BEST course of action to maintain application health?

A. Manually scale up the Auto Scaling group associated with the ALB.

B. Increase the health check timeout value for the ALB to give instances more time to respond.

C. Enable connection draining on the ALB to gracefully remove unhealthy instances.

D. Implement a scaling policy in the Auto Scaling group to automatically scale based on traffic metrics

40. You have a public-facing web server in a VPC (Virtual Private Cloud) running on an EC2 instance in a public subnet. You also have a private MySQL database in a private subnet. The web server needs to access the database to retrieve data.

A. In the web server's security group, allow inbound HTTP traffic from anywhere (0.0.0.0/0) on port 80 and outbound traffic to the database's security group on port 3306.In the database's security group, allow inbound traffic from the web server's security group IP address on port 3306.

B. In the web server's security group, allow inbound HTTP traffic from anywhere (0.0.0.0/0) on port 80. In the database's security group, allow inbound traffic from anywhere (0.0.0.0/0) on port 3306.

C. In the web server's security group, allow inbound HTTP traffic from anywhere (0.0.0.0/0) on port 80 and outbound traffic to the database's security group on port 3306. In the database's security group, only allow inbound traffic from the web server's specific IP address on port 3306.

D. Create a security group for the web server and database communication. Allow inbound HTTP traffic to the web server on port 80 and outbound traffic on the designated communication port to the database security group. In the database security group, only allow inbound traffic from the communication security group on the designated port.

**Explain the difference between EBS and S3.**

**Explain failover routing in Route 53 and its integration with Load Balancers.**

**Explain AWS Lambda functions with an example scenario.**

**My application is running inside a private EC2 instance. How can the server connect to S3 privately?**

**What is the necessity of monitoring in Cloud and DevOps?**