When working with Amazon RDS, by default AWS is responsible for implementing which two management-related activities? (Pick 2 correct answers)

A. Importing data and optimizing queries
B. Installing and periodically patching the database software
C. Creating and maintaining automated database backups with a point-in-time recovery of up to five minutes
D. Creating and maintaining automated database backups in compliance with regulatory long-term retention requirements

You maintain an application on AWS to provide development and test platforms for your developers. Currently both environments consist of an m1.small EC2 instance. Your developers notice performance degradation as they increase network load in the test environment.

How would you mitigate these performance issues in the test environment?

A. Upgrade the m1.small to a larger instance type
B. Add an additional ENI to the test instance
C. Use the EBS optimized option to offload EBS traffic
D. Configure Amazon Cloudwatch to provision more network bandwidth when network utilization exceeds 80%

Per the AWS Acceptable Use Policy, penetration testing of EC2 instances:

A. may be performed by the customer against their own instances, only if performed from EC2 instances.
B. may be performed by AWS, and is periodically performed by AWS.
C. may be performed by AWS, and will be performed by AWS upon customer request.
D. are expressly prohibited under all circumstances.
E. may be performed by the customer against their own instances with prior authorization from AWS.

You have been tasked with identifying an appropriate storage solution for a NoSQL database that requires random I/O reads of greater than 100,000 4kB IOPS.

Which EC2 option will meet this requirement?

A. EBS provisioned IOPS
B. SSD instance store
C. EBS optimized instances
D. High Storage instance configured in RAID 10

Instance A and instance B are running in two different subnets A and B of a VPC. Instance A is not able to ping instance B.

What are two possible reasons for this? (Pick 2 correct answers)

A. The routing table of subnet A has no target route to subnet B
B. The security group attached to instance B does not allow inbound ICMP traffic
C. The policy linked to the IAM role on instance A is not configured correctly
D. The NACL on subnet B does not allow outbound ICMP traffic

Your web site is hosted on 10 EC2 instances in 5 regions around the globe with 2 instances per region.

How could you configure your site to maintain site availability with minimum downtime if one of the 5 regions was to lose network connectivity for an extended period of time?

A. Create an Elastic Load Balancer to place in front of the EC2 instances. Set an appropriate health check on each ELB.
B. Establish VPN Connections between the instances in each region. Rely on BGP to failover in the case of a region wide connectivity outage
C. Create a Route 53 Latency Based Routing Record Set that resolves to an Elastic Load Balancer in each region. Set an appropriate health check on each ELB.
D. Create a Route 53 Latency Based Routing Record Set that resolves to Elastic Load Balancers in each region and has the Evaluate Target Health flag set to true.

You run a stateless web application with the following components: Elastic Load Balancer (ELB), 3 Web/Application servers on EC2, and 1 MySQL RDS database with 5000 Provisioned IOPS. Average response time for users is increasing. Looking at CloudWatch, you observe 95% CPU usage on the Web/Application servers and 20% CPU usage on the database. The average number of database disk operations varies between 2000 and 2500.

Which two options could improve response times? (Pick 2 correct answers)

A. Choose a different EC2 instance type for the Web/Application servers with a more appropriate CPU/memory ratio
B. Use Auto Scaling to add additional Web/Application servers based on a CPU load threshold
C. Increase the number of open TCP connections allowed per web/application EC2 instance
D. Use Auto Scaling to add additional Web/Application servers based on a memory usage threshold

Which features can be used to restrict access to data in S3? (Pick 2 correct answers)

A. Create a CloudFront distribution for the bucket.
B. Set an S3 bucket policy.
C. Use S3 Virtual Hosting.
D. Set an S3 ACL on the bucket or the object.
E. Enable IAM Identity Federation.

You need to establish a backup and archiving strategy for your company using AWS. Documents should be immediately accessible for 3 months and available for 5 years for compliance reasons.

Which AWS service fulfills these requirements in the most cost effective way?

A. Use StorageGateway to store data to S3 and use life-cycle policies to move the data into Redshift for long-time archiving
B. Use DirectConnect to upload data to S3 and use IAM policies to move the data into Glacier for long-time archiving
C. Upload the data on EBS, use life-cycle policies to move EBS snapshots into S3 and later into Glacier for long-time archiving
D. Upload data to S3 and use life-cycle policies to move the data into Glacier for long-time archiving

Given the following IAM policy:

```
{
"Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",  "s3:List*"
        ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::corporate_bucket/*"
    }
  ]
}
```

What does the IAM policy allow? (Pick 3 correct answers)

A. The user is allowed to read objects from all S3 buckets owned by the account
B. The user is allowed to write objects into the bucket named 'corporate_bucket'
C. The user is allowed to change access rights for the bucket named 'corporate_bucket'
D. The user is allowed to read objects in the bucket named 'corporate_bucket' but not allowed to list the objects in the bucket
E. The user is allowed to read objects from the bucket named 'corporate_bucket'