1) A company is migrating a legacy web application from a single server to multiple Amazon EC2 instances behind an Application Load Balancer (ALB). After the migration, users report that they are frequently losing their sessions and are being prompted to log in again.

Which action should be taken to resolve the issue reported by users?

A) Confirm that the ALB is not in a Multi-AZ configuration.
B) Configure an Amazon CloudFront distribution with the ALB as the origin.
C) Deploy a Network Load Balancer in front of the ALB.
D) Enable sticky sessions for the target group of EC2 instances.

2) A sysops team checks their AWS Personal Health Dashboard every week for upcoming AWS hardware maintenance events. Recently, a team member was on vacation and the team missed an event, which resulted in an outage. The team wants a simple method to ensure that everyone is aware of upcoming events without depending on an individual team member checking the dashboard.

What should be done to address this?

A) Build a web scraper to monitor the Personal Health Dashboard. When new health events are detected, send a notification to an Amazon SNS topic monitored by the entire team.
B) Create an Amazon CloudWatch Events event based off the AWS Health service and send a notification to an Amazon SNS topic monitored by the entire team.
C) Create an Amazon CloudWatch Events event that sends a notification to an Amazon SNS topic monitored by the entire team to remind the team to view the maintenance events on the Personal Health Dashboard.
D) Create an AWS Lambda function that continuously pings all EC2 instances to confirm their health. Alert the team if this check fails.

3) An application running in a VPC needs to access instances owned by a different account and running in a VPC in a different AWS Region. For compliance purposes, the traffic must not traverse the public internet.

How should a sysops administrator configure network routing to meet these requirements?

A) Within each account, create a custom routing table containing routes that point to the other account's virtual private gateway.
B) Within each account, set up a NAT gateway in a public subnet in its respective VPC. Then, using the public IP address from the NAT gateway, enable routing between the two VPCs.
C) From one account, configure a Site-to-Site VPN connection between the VPCs. Within each account, add routes in the VPC route tables that point to the CIDR block of the remote VPC.
D) From one account, create a VPC peering request. After an administrator from the other account accepts the request, add routes in the route tables for each VPC that point to the CIDR block of the peered VPC.

4) An application running on Amazon EC2 instances needs to access data stored in an Amazon DynamoDB table.

Which solution will grant the application access to the table in the MOST secure manner?

A) Create an IAM group for the application and attach a permissions policy with the necessary privileges. Add the EC2 instances to the IAM group.
B) Create an IAM resource policy for the DynamoDB table that grants the necessary permissions to Amazon EC2.
C) Create an IAM role with the necessary privileges to access the DynamoDB table. Associate the role with the EC2 instances.
D) Create an IAM user for the application and attach a permissions policy with the necessary privileges. Generate an access key and embed the key in the application code.

5) A third-party service uploads objects to Amazon S3 every night. Occasionally, the service uploads an incorrectly formatted version of an object. In these cases, the sysops administrator needs to recover an older version of the object.

What is the MOST efficient way to recover the object without having to retrieve it from the remote service?

A) Configure an Amazon CloudWatch Events scheduled event that triggers an AWS Lambda function that backs up the S3 bucket prior to the nightly job. When bad objects are discovered, restore the backed up version.
B) Create an S3 event on object creation that copies the object to an Amazon Elasticsearch Service (Amazon ES) cluster. When bad objects are discovered, retrieve the previous version from Amazon ES.
C) Create an AWS Lambda function that copies the object to an S3 bucket owned by a different account. Trigger the function when new objects are created in Amazon S3. When bad objects are discovered, retrieve the previous version from the other account.
D) Enable versioning on the S3 bucket. When bad objects are discovered, access previous versions with the AWS CLI or AWS Management Console.

6) According to the AWS shared responsibility model, for which of the following Amazon EC2 activities is AWS responsible? (Select TWO.)

A) Configuring network ACLs
B) Maintaining network infrastructure
C) Monitoring memory utilization
D) Patching the guest operating system
E) Patching the hypervisor

7) A security and compliance team requires that all Amazon EC2 workloads use approved Amazon Machine Images (AMIs). A sysops administrator must implement a process to find EC2 instances launched from unapproved AMIs.

Which solution will meet these requirements?

A) Create a custom report using AWS Systems Manager inventory to identify unapproved AMIs.
B) Run Amazon Inspector on each EC2 instance and flag the instance if it is using unapproved AMIs.
C) Use an AWS Config rule to identify unapproved AMIs.
D) Use AWS Trusted Advisor to identify the EC2 workloads using unapproved AMIs.

8) A sysops administrator observes a large number of rogue HTTP requests on an Application Load Balancer. The requests originate from various IP addresses. These requests cause increased server load and costs.

What should the administrator do to block this traffic?

A) Install Amazon Inspector on Amazon EC2 instances to block the traffic.
B) Use Amazon GuardDuty to protect the web servers from bots and scrapers.
C) Use AWS Lambda to analyze the web server logs, detect bot traffic, and block the IP addresses in the security groups.
D) Use an AWS WAF rate-based rule to block the traffic when it exceeds a threshold.

9) A sysops administrator is implementing security group policies for a web application running on AWS. An Elastic Load Balancer connects to a fleet of Amazon EC2 instances that connect to an Amazon RDS database over port 1521. The security groups are named elbSG, ec2SG, and rdsSG, respectively.

How should these security groups be implemented?

A) elbSG: allow port 80 and 443 from 0.0.0.0/0;
ec2SG: allow port 443 from elbSG;
rdsSG: allow port 1521 from ec2SG.

B) elbSG: allow port 80 and 443 from 0.0.0.0/0;
ec2SG: allow port 80 and 443 from elbSG and rdsSG;
rdsSG: allow port 1521 from ec2SG.

C) elbSG: allow port 80 and 443 from ec2SG;
ec2SG: allow port 80 and 443 from elbSG and rdsSG;
rdsSG: allow port 1521 from ec2SG.

D) elbSG: allow port 80 and 443 from ec2SG;
ec2SG: allow port 443 from elbSG;
rdsSG: allow port 1521 from elbSG.

10) An ecommerce company wants to lower costs on its nightly jobs that aggregate the current day's sales and store the results in Amazon S3. The jobs run on multiple On-Demand Instances, and the jobs take just under 2 hours to complete. The jobs can run at any time during the night. If the job fails for any reason, it needs to be started from the beginning.

Which solution is the MOST cost-effective based on these requirements?

A) Purchase Reserved Instances.
B) Submit a request for a Spot block.
C) Submit a request for all Spot Instances.
D) Use a mixture of On-Demand and Spot Instances.

Answers

1) D – Legacy applications designed to run on a single server frequently store session data locally. When these applications are deployed on multiple instances behind a load balancer, user requests are routed to instances using the round robin routing algorithm. Session data stored on one instance would not be present on the others. By enabling sticky sessions, cookies are used to track user requests and keep subsequent requests going to the same instance.

2) B – The AWS Health service publishes Amazon CloudWatch Events. CloudWatch Events can trigger Amazon SNS notifications. This method requires neither additional coding nor infrastructure. It automatically notifies the team of upcoming events, and does not depend upon brittle solutions like web scraping.

3) D – A VPC peering connection enables routing using each VPC's private IP addresses as if they were in the same network. Traffic using inter-Region VPC peering always stays on the global AWS backbone and never traverses the public internet.

4) C - An IAM role can be used to provide permissions for applications that are running on Amazon EC2 instances to make AWS API requests using temporary credentials.

5) D – Enabling versioning is a simple solution; (A) involves writing custom code, (C) has no versioning, so the replication will overwrite the old version with the bad version if the error is not discovered quickly, and (B) will involve expensive storage that is not well suited for objects.

6) B, E – AWS provides security of the cloud, including maintenance of the hardware and hypervisor software supporting Amazon EC2. Customers are responsible for any maintenance or monitoring within an EC2 instance, and for configuring their VPC infrastructure.

7) C – AWS Config has a managed rule that handles this scenario.

8) D – AWS WAF has rules that can protect web applications from HTTP flood attacks.

9) A – elbSG must allow all web traffic (HTTP and HTTPS) from the internet. ec2SG must allow traffic from the load balancer only, in this case identified as traffic from elbSG. The database must allow traffic from the EC2 instances only, in this case identified as traffic from ec2SG.

10) B – The solution will take advantage of Spot pricing, but by using a Spot block instead of Spot Instances, the company can be assured the job will not be interrupted.