Practice Exam 2

10 Questions, 20 Minutes

Question 1

You are migrating a business-to-business application to AWS. The application uses a client-server architecture, and the server side consists of application servers and a relational database. All communication is via HTTPS. Client systems each have a client certificate and use SSL mutual authentication to uniquely identify the client to the application tier. To maximize availability and minimize costs, you plan to implement the application tier as an Auto Scaling group behind an ELB load balancer.

During migration planning, you find that the server side also initiates communication with the client systems. This requires the Application servers to know the IP address of the client in order to initiate outbound communications. You are able to make changes to the solution architecture and can also make changes to the application code. What should you do to maintain high availability while allowing communication to the client systems?

A Configure the load balancer with an SSL listener, load the client certificates into the certificate store in IAM, and use the SSL listener on the load balancer to handle the mutual authentication.

B Implement Proxy Protocol support on the load balancer. Change the application to use the Proxy Protocol information to get the source IP address of the client systems. Terminate SSL connections on the load balancer.

C Implement Proxy Protocol support on the load balancer. Change the application to use the Proxy Protocol information to get the source IP address of the client systems. Terminate SSL connections on the application servers.

D Remove the load balancer from the architecture and terminate the SSL connections directly on the application servers. Manually create an Amazon Route 53 Weighted Round Robin record set that lists all of the application servers. Create a Route 53 health check.

Question 2

You lead the new Operations team at your company. You plan to use Amazon Elastic Compute Cloud (EC2) and Amazon Virtual Private Cloud (VPC) to provide environments for your developers to work on new versions of your in-house applications. Your marketing department has been running several high-profile workloads for the last nine months, also in the same AWS account. You need to ensure that your team can create new instances while not disturbing the marketing workloads. You have created IAM users for your team. What should you do next?

A Apply an IAM role to the Operations team users. Allow the role to launch new EC2 instances, and deny the role permission to terminate Marketing EC2 instances.

B Allow Operations team users to launch new EC2 instances. Enable EC2 Termination Protection for the Marketing EC2 instances to prevent your team from terminating them.

C Enable multi-factor authentication for Operations team IAM users, to require the Operations team to authenticate before terminating the Marketing EC2 instances.

D Use resource-based tagging. Create an IAM policy that prevents Operations team users from creating tags and prevents the team from terminating EC2 instances with a tag where Department = Marketing.

Question 3

Your mobile application launched recently and has seen a surge in popularity over the last month. The mobile application talks directly to your API servers, which are configured in an Auto Scaling group. A multi-AZ Amazon Relational Database Service (RDS) instance stores all data. Most of the database transactions are reads. CloudWatch shows that the CPU of the database regularly hits 80% during more complex reads. What should you do to ensure performance and high availability of your application as demand grows?

A Increase the Auto Scaling maximum. Because the database is already multi-AZ, no other action is required.

B Add two Amazon ElastiCache memcached instances in different Availability Zones. Configure the API servers to cache read results in both ElastiCache instances, and check the ElastiCache instances for results before querying the database.

C Add one ElastiCache memcached instance. Configure the API servers to cache read results in the ElastiCache instance, and check the ElastiCache instance for results before querying the database.

D Add an RDS Read Replica. Configure your application to read from the Read Replica.

Question 4

Your organization uses a variety of EC2 instances across the m4, c4, and r3 families. You recently purchased a number of m4.xlarge Reserved Instances. You want to ensure that people are using these reservations wherever practical, so you want a way to track who has launched an instance and what instance types are running. What should you do?

A Create a scheduled task to run *ec2-describe-instances* every hour. Filter the responses by AWS Identity and Access Management (IAM) user to identify owners of instances that are not covered by the Reserved Instance purchase.

B Create an AWS CloudFormation custom resource that sends notifications to an Amazon Simple Notification Service (SNS) topic, containing information from an instance launch. Alter your CloudFormation templates to include the custom resource, and set the DependsOn parameter so that all EC2 instances in the template depend on the custom resource. Use the information to determine the owners of instances that are not covered by the Reserved Instance purchase.

C Create an IAM policy with a Condition that only allows users to launch m4.xlarge instances. Add this policy to all of your IAM groups. Use Cost Explorer to determine which users are running other instance types.

D Create a tagging scheme that includes the name of the person launching the instance. Periodically run *ec2-describe-instances* and use the tags to identify owners of instances not covered by your reserved instances.

Question 5

Your company runs a popular music review site. The front end is composed of three Auto Scaling groups with thousands of instances in each. The instances reside in one VPC in the US-EAST-1 region. You have been asked to design and implement an intrusion prevention system for these instances. How should you design this?

A Create an Auto Scaling group of monitoring instances. Install a software agent on all front-end instances. Have the software agent collect traffic and send to the monitoring systems for inspection.

B Configure one monitoring instance in each Availability Zone. Attach an Elastic Network Interface for each subnet in that Availability Zone, and use promiscuous mode to sniff all the traffic within each subnet.

C Create monitoring instances in each public subnet within the VPC. Configure the default route table with a default route that sends all traffic to the monitoring instances. Remove all other route tables.

D Create another VPC that contains only the intrusion prevention system. Edit the route tables in the production VPC to send all traffic to the monitoring systems in the new VPC.

Question 6

Your company created a mobile-optimized site for people to leave quick, anonymous reviews of places and events. These reviews are only shown for 24 hours and are then removed. The site is written in JavaScript so it runs on the broadest range of devices.

Because the reviews are very small, you have decided to store the reviews in Amazon Kinesis and process them with AWS Lambda. How should you provide credentials for the mobile site to put items into the Amazon Kinesis stream?

A Create a role with permissions to put data into the Amazon Kinesis stream. Use Amazon Cognito with unauthenticated identities. Use the JavaScript SDK and Amazon Cognito to retrieve temporary credentials. Use these temporary credentials to put reviews into the Amazon Kinesis stream.

B Create a role with permissions to put data into the Amazon Kinesis stream. Use Amazon Cognito. Have users sign in via Facebook, Google, or Login with Amazon. Use the JavaScript SDK and Amazon Cognito to retrieve temporary credentials. Use these temporary credentials to put reviews into the Kinesis stream.

C Create an IAM user with permissions to put data into the Amazon Kinesis stream. Generate an access key and secret access key. Put these in an S3 bucket, and have the JavaScript site retrieve the keys from the S3 bucket. Rotate the keys daily.

D Create a role with permissions to put data into the Amazon Kinesis stream and execute Lambda functions. Use Amazon Cognito with unauthenticated identities. Use the JavaScript SDK and Amazon Cognito to retrieve temporary credentials. Use these temporary credentials to put reviews into the Amazon Kinesis stream and then execute the Lambda functions.

Question 7

Your company's SaaS service allows organizations to manage their shift-worker schedules, time off, conflict detection, and automated resolution. A new service will offer predictive scheduling based on historical information. This will allow your customers to better plan for daily, weekly, and seasonal demand. The predictive scheduling engine will run once per week on a Sunday night and will produce per-customer reports covering the next four weeks.

You started with a small proof of concept environment in your existing facilities. This shows that the work is very compute-intensive, but is also very parallelizable because each customer's information is independent. As you expand the offering to a larger portion of your customers, you will need more and more compute power to ensure that the reports are completed in a timely fashion.

The source data is in a large relational database in your on-premises facilities. Because of the data volume and rate of change, you plan to continually replicate data to a read-only database server on AWS.

You need to create a solution that will allow you to run the prediction engine on AWS while retaining the master copy of the data in your facilities. What should you recommend?

A Create a single CloudFormation template. The template will include a VPC, a VPN connection to your facilities, and an Auto Scaling group that launches from a custom AMI with the prediction engine software pre-installed. Create this stack each week, and delete the stack on completion of the predictions.

B Create a CloudFormation template to provision a VPC and VPN connection. Create a stack from this template and leave it in CREATE_COMPLETE state. Create a separate CloudFormation template containing an Auto Scaling group that launches from a custom AMI with the prediction engine software pre-installed. Create a stack from this template each week, and delete the stack on completion of the predictions.

C Create a CloudFormation template to provision a VPC and VPN connection. Create a template containing an Auto Scaling group that launches from a custom AMI with the prediction engine software pre-installed. Nest the second template in the first template using the AWS::CloudFormation::Stack resource type. Create a stack from the first template and leave it in CREATE_COMPLETE state.

D Create a CloudFormation template for each customer. The template will include a VPC, a VPN connection to your facilities, and an Auto Scaling group that launches from a custom AMI with the prediction engine software pre-installed. Create a stack for each customer each week. Delete each stack on completion of the predictions.

Question 8

Your company created a new division specifically to experiment with new ideas and deliver innovative services. Another architect created several Virtual Private Clouds (VPCs) using the AWS Console; however, teams have started requesting the ability to deploy their own VPCs on demand. You have decided to use CloudFormation to standardize creation of VPCs and enable teams to deploy them on demand.

Your security policy requires that application and database servers do not have direct access to the Internet, but web servers can have direct Internet access. To help meet this requirement, your CloudFormation template creates two subnets for each Availability Zone: one public, one private. What else should you do in the CloudFormation template to maximize availability?

A Create a NAT instance in one subnet. Create a route table with the NAT instance as the target for the 0.0.0.0/0 route. Associate that route table with all subnets.

B Create a CloudFormation Condition called “isPrivate” and in each Availability Zone, create a NAT instance in the private subnet. Create a route table with the NAT instance as the target for the 0.0.0.0/0 route. Associate that route table with the subnets where the “isPrivate” condition is true.

C Create NAT instances in each public subnet. Create a route table with all NAT instances as targets for the 0.0.0.0/0 route. Associate that route table with the private subnets. Create another route table with an Internet gateway as the target for the 0.0.0.0/0 route. Associate that route table with the public subnets.

D Create an Internet gateway in one subnet. Create a route table with the Internet gateway as the target for the 0.0.0.0/0 route. Associate that route table with all subnets.

E In each Availability Zone, create a NAT instance in the public subnet and a route table with that NAT instance as the target for the 0.0.0.0/0 route. Associate that route table with the private subnet. Create another route table for each Availability Zone, with the Internet gateway as the target for the 0.0.0.0/0 route. Associate that route table with the public subnet in that Availability Zone.

Question 9

You created a database server on an EC2 instance. Because you are expecting high volumes of both read and write traffic to the database, you have attached four 1-TB Amazon Elastic Block Store (EBS) Provisioned IOPS volumes, each with 10,000 IOPS provisioned. Within the operating system, you created a RAID-0 stripe set across the four EBS volumes, with a 16-KB stripe size. In initial performance testing, you cannot saturate the IO to the volumes. What is causing the problem, and what is the solution?

A The EC2 instance is not EBS-optimized. Change the instance to an EBS-optimized instance with sufficient throughput to handle the IOPS required.

B RAID-0 cannot scale to handle high IOPS. Change the RAID layout to a RAID-5 set.

C The 16-KB stripe size is causing the performance bottleneck. Remove the RAID-0 stripe and recreate a new RAID-0 stripe with a 16-MB stripe size.

D The EC2 instance is not using a placement group. Change the instance to launch in a placement group to provide sufficient throughput to handle the IOPS required.

E The queue depth settings being used in the test utility are too small. Change the queue depth settings from 16 to at least 1024.

Question 10

Your company produces remotely controlled industrial automation robots for use in high-risk environments. The new generation of robots will feature a function that records the position, direction, and speed of the unit and sends this data to your company for analysis. Each unit will send this information every five seconds, and the designers have formatted the information into a JSON object. You are designing the back-end systems that will receive this data and process it. The goal is to provide real-time information back to the teams controlling the robots. What architecture should you use?

A Have each unit post the data to a common S3 bucket. Configure S3 event notifications on the bucket. When a new item is posted to the bucket, create an Elastic Beanstalk worker tier to process the results. Send recommendation information to the control teams directly.

B Have each unit post the data to an Amazon Simple Queue Service (SQS) queue. Configure an Elastic Beanstalk worker tier to analyze the data and store recommendations in an RDS MySQL database. Periodically create another Elastic Beanstalk worker tier to read the recommendations and send to the control teams using Amazon Simple Email Service (SES).

C Have each unit post the data to an Amazon Kinesis stream. Use an autoscaling group of EC2 instances with the Amazon Kinesis Client Library to process the information, sending recommendation information to the control teams directly.

D Have each unit post the data directly to an Amazon DynamoDB table. Use DynamoDB triggers to trigger a Lambda function to analyze the data. Have the Lambda function place the recommendation information on a website for the control teams to view.

Answers are listed on the next page

Answers

1	C
2	D
3	B
4	D
5	A
6	A
7	B
8	E
9	A
10	C