1) A company has many AWS accounts that individual business groups own. One of the accounts was recently compromised. The attacker launched a large number of instances, resulting in a high bill for that account.

The company addressed the security breach, but a solutions architect needs to develop a solution to prevent excessive spending in all accounts. Each business group wants to retain full control of its AWS account.

Which solution should the solutions architect recommend to meet these requirements?

A) Use AWS Organizations. Add each AWS account to the management account. Create an SCP that uses the ec2:instanceType condition key to prevent the launch of high-cost instance types in each account.
B) Attach a new customer-managed IAM policy to an IAM group in each account. Configure the policy to use the ec2:instanceType condition key to prevent the launch of high-cost instance types. Place all the existing IAM users in each group.
C) Turn on billing alerts for each AWS account. Create Amazon CloudWatch alarms that send an Amazon Simple Notification Service (Amazon SNS) notification to the account administrator whenever the account exceeds a designated spending threshold.
D) Turn on AWS Cost Explorer in each account. Review the Cost Explorer reports for each account on a regular basis to ensure that spending does not exceed the desired amount.

2) A company has multiple AWS accounts in an organization in AWS Organizations. The company has integrated its on-premises Active Directory with AWS Single Sign-On (AWS SSO) to grant Active Directory users least privilege permissions to manage infrastructure across all the accounts.

A solutions architect must integrate a third-party monitoring solution that requires read-only access across all AWS accounts. The monitoring solution will run in its own AWS account.

What should the solutions architect do to provide the monitoring solution with the required permissions?

A) Create a user in an AWS SSO directory. Assign a read-only permissions set to the user. Assign all AWS accounts that need monitoring to the user. Provide the third-party monitoring solution with the user name and password.
B) Create an IAM role in the organization's management account. Allow the AWS account of the third-party monitoring solution to assume the role.
C) Invite the AWS account of the third-party monitoring solution to join the organization. Enable all features.
D) Create an AWS CloudFormation template that defines a new IAM role for the third-party monitoring solution. Specify the AWS account of the third-party monitoring solution in the trust policy. Create the IAM role across all linked AWS accounts by using a stack set.

3) A team is building an HTML form that is hosted in a public Amazon S3 bucket. The form uses JavaScript to post data to an Amazon API Gateway API endpoint. The API endpoint is integrated with AWS Lambda functions. The team has tested each method in the API Gateway console and has received valid responses.

Which combination of steps must the team complete so that the form can successfully post to the API endpoint and receive a valid response? (Select TWO.)

A) Configure the S3 bucket to allow cross-origin resource sharing (CORS).
B) Host the form on Amazon EC2 rather than on Amazon S3.
C) Request a quota increase for API Gateway.
D) Enable cross-origin resource sharing (CORS) in API Gateway.
E) Configure the S3 bucket for web hosting.

4) A company runs a serverless mobile app that uses Amazon API Gateway, AWS Lambda functions, Amazon Cognito, and Amazon DynamoDB. During large surges in traffic, users report intermittent system failures. The API Gateway API endpoint is returning HTTP status code 502 (Bad Gateway) errors to valid requests.

Which solution will resolve this issue?

A) Increase the concurrency quota for the Lambda functions. Configure Amazon CloudWatch to send notification alerts when the ConcurrentExecutions metric approaches the quota.
B) Configure notification alerts for the quota of transactions per second on the API Gateway API endpoint. Create a Lambda function that will increase the quota when the quota is reached.
C) Shard users to Amazon Cognito user pools in multiple AWS Regions to reduce user authentication latency.
D) Use DynamoDB strongly consistent reads to ensure that the client application always receives the most recent data.

5) A company is launching a new web service on an Amazon Elastic Container Service (Amazon ECS) cluster. The cluster consists of 100 Amazon EC2 instances. Company policy requires the security group on the cluster instances to block all inbound traffic except HTTPS (port 443).

Which solution will meet these requirements?

A) Change the SSH port to 2222 on the cluster instances by using a user data script. Log in to each instance by using SSH over port 2222.
B) Change the SSH port to 2222 on the cluster instances by using a user data script. Use AWS Trusted Advisor to remotely manage the cluster instances over port 2222.
C) Launch the cluster instances with no SSH key pairs. Use AWS Systems Manager Run Command to remotely manage the cluster instances.
D) Launch the cluster instances with no SSH key pairs. Use AWS Trusted Advisor to remotely manage the cluster instances.

6) A company has two AWS accounts: one account for production workloads and one account for development workloads. A development team and an operations team create and manage these workloads. The company needs a security strategy that meets the following requirements:

- **Developers need to create and delete development application infrastructure.**
- **Operators need to create and delete development and production application infrastructure.**
- **Developers must have no access to production infrastructure.**
- **All users must have a single set of AWS credentials.**

Which strategy will meet these requirements?

A) In the production account:
- Create an operations IAM group that can create and delete application infrastructure.
- Create an IAM user for each operator. Assign these users to the operations group.

In the development account:
- Create a development IAM group that can create and delete application infrastructure.
- Create an IAM user for each operator and developer. Assign these users to the development group.

B) In the production account:
- Create an operations IAM group that can create and delete application infrastructure.

In the development account:
- Create a development IAM group that can create and delete application infrastructure.
- Create an IAM user for each developer. Assign these users to the development group.
- Create an IAM user for each operator. Assign these users to the development group and to the operations group in the production account.

C) In the development account:
- Create a shared IAM role that can create and delete application infrastructure in the production account.
- Create a development IAM group that can create and delete application infrastructure.
- Create an operations IAM group that can assume the shared role.
- Create an IAM user for each developer. Assign these users to the development group.
- Create an IAM user for each operator. Assign these users to the development group and to the operations group.

D) In the production account:
- Create a shared IAM role that can create and delete application infrastructure.
- Add the development account to the trust policy for the shared role.

In the development account:
- Create a development IAM group that can create and delete application infrastructure.
- Create an operations IAM group that can assume the shared role in the production account.
- Create an IAM user for each developer. Assign these users to the development group.
- Create an IAM user for each operator. Assign these users to the development group and to the operations group.

7) A solutions architect needs to reduce costs for a big data application. The application environment consists of hundreds of devices that send events to Amazon Kinesis Data Streams. The device ID is used as the partition key, so each device gets a separate shard. Each device sends between 50 KB and 450 KB of data each second. An AWS Lambda function polls the shards, processes the data, and stores the result in Amazon S3.

Every hour, another Lambda function runs an Amazon Athena query against the result data to identify outliers. This Lambda function places the outliers in an Amazon Simple Queue Service (Amazon SQS) queue. An Amazon EC2 Auto Scaling group of two EC2 instances monitors the queue and runs a 30-second process to address the outliers. The devices submit an average of 10 outlying values every hour.

Which combination of changes to the application will MOST reduce costs? (Select TWO.)

A) Change the Auto Scaling group launch configuration to use smaller instance types in the same instance family.
B) Replace the Auto Scaling group with a Lambda function that is invoked when messages arrive in the queue.
C) Reconfigure the devices and data stream to set a ratio of 10 devices to 1 data stream shard.
D) Reconfigure the devices and data stream to set a ratio of 2 devices to 1 data stream shard.
E) Change the desired capacity of the Auto Scaling group to a single EC2 instance.

8) A company operates an ecommerce application on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. After an order is successfully processed, the application immediately posts order data to a third-party affiliate's external tracking system that pays sales commissions for order referrals.

During a successful marketing promotion, the number of EC2 instances increased from 2 to 20. The application continued to work correctly during this time. However, the increased request rate overwhelmed the third-party affiliate and resulted in failed requests.

Which combination of architectural changes should a solutions architect make to ensure that the entire process functions correctly under load? (Select TWO.)

A) Move the code that calls the affiliate to a new AWS Lambda function. Modify the application to invoke the Lambda function asynchronously.
B) Move the code that calls the affiliate to a new AWS Lambda function. Modify the application to place the order data in an Amazon Simple Queue Service (Amazon SQS) queue. Invoke the Lambda function from the queue.
C) Increase the timeout of the new AWS Lambda function.
D) Decrease the reserved concurrency of the new AWS Lambda function.
E) Increase the memory of the new AWS Lambda function.

9) A company has built an online ticketing web application on AWS. The application is hosted on AWS App Runner and uses images that are stored in an Amazon Elastic Container Registry (Amazon ECR) repository. The application stores data in an Amazon Aurora MySQL DB cluster. The company has set up a domain name in Amazon Route 53.

The company needs to deploy the application across two AWS Regions in an active-active configuration.

Which combination of steps will meet these requirements with the LEAST change to the architecture? (Select THREE.)

A) Set up Cross-Region Replication to the second Region for the ECR images.
B) Create a VPC endpoint from the ECR repository in the second Region.
C) Edit the App Runner configuration by adding a second deployment target to the second Region.
D) Deploy App Runner to the second Region. Set up Route 53 latency-based routing.
E) Change the database by using Amazon DynamoDB global tables in the two desired Regions.
F) Use an Aurora global database with write forwarding enabled in the second Region.

10) A company has deployed a multi-tier web application in the AWS Cloud. The application consists of the following tiers:

- **A Windows-based web tier that is hosted on Amazon EC2 instances with Elastic IP addresses**
- **A Linux-based application tier that is hosted on EC2 instances that run behind an Application Load Balancer (ALB) that uses path-based routing**
- **A MySQL database that runs on a Linux EC2 instance**

All the EC2 instances are using Intel-based x86 CPUs. A solutions architect needs to modernize the infrastructure to achieve better performance. The solution must minimize the operational overhead of the application.

Which combination of actions should the solutions architect take to meet these requirements? (Select TWO.)

A) Run the MySQL database on multiple EC2 instances.
B) Place the web tier instances behind an ALB.
C) Migrate the MySQL database to Amazon Aurora Serverless.
D) Migrate all EC2 instance types to Graviton2.
E) Replace the ALB for the application tier instances with a company-managed load balancer.

Answers

1) C – Billing alarms will provide the company with alerts about excessive spending without taking away control from any of the business groups. Options A and B are incorrect because each business group wants to retain control of its account. These options would not prevent the launch of a large number of instances. Option D is a manual process that would not provide immediate alerts about excessive spending.

2) D – AWS CloudFormation StackSets can deploy the IAM role across multiple accounts with a single operation. Option A is incorrect because credentials that are supplied by AWS Single Sign-On (AWS SSO) are temporary. The application would lose permissions and would have to log in again. Option B would grant access to the management account only. Option C is incorrect because when an account joins an organization, the account does not receive permissions to access the other accounts in the organization.

3) D, E – Cross-origin resource sharing (CORS) is a browser security feature that restricts HTTP requests that initiate from scripts that run in the browser. CORS is typically required to build web applications that access APIs that are hosted on a different domain or origin. You can enable CORS to allow requests to your API from a web application that is hosted on a different domain. For example, if your API is hosted on https://[api_id].execute-api.[region].amazonaws.com/ and you want to call your API from a web application that is hosted on [bucketname].s3.website-[region], your API must support CORS. Option E is required for the HTML form to be served through a website endpoint.

Option A is incorrect because the CORS header must be configured to be returned by the dynamic response from the API endpoint. The configuration of CORS for the S3 bucket does not help. Option B is incorrect because there is no advantage to serving a static webpage from a web server that runs on Amazon EC2 instead of from an S3 bucket. Option C is incorrect because API Gateway has a default quota of 10,000 requests per second for each AWS Region. If necessary, you can increase this quota.

4) A – Amazon API Gateway will intermittently return HTTP status code 502 (Bad Gateway) errors if the AWS Lambda function exceeds its concurrency quota. Option B is incorrect because, in this case, API Gateway would return a status code 429 error for too many requests. Option C is incorrect because the errors occur during calls to the API Gateway API endpoint, not during the authentication process. Option D is incorrect because stale data would not cause a Bad Gateway error.

5) C – AWS Systems Manager Run Command requires no inbound ports to be open. Run Command operates entirely over outbound HTTPS, which is open by default for security groups. Options A and B are incorrect because the requirements state that the only inbound port that should be open is 443. Option D is incorrect because AWS Trusted Advisor does not perform this management function.

6) D – The correct answer follows the standard guidelines for granting cross-account access between two accounts that you control. Option A does not meet the requirements because it requires two sets of credentials for operators. Option B is incorrect because you cannot add an IAM user to an IAM group in a different account. Option C is incorrect because a role cannot grant access to resources in another account. The shared role must be in the same account with resources that the shared role manages.

7) B, D – The average amount of compute to address the outliers each hour is 300 seconds (10 events for 30 seconds each). Option B is correct because with AWS Lambda, you pay only for the small amount of compute time that is required to process the outlying values. While options A and E would reduce costs, they both involve paying for one or more Amazon EC2 instances that would sit unused for 3,300 seconds each hour. Options C and D reduce the shard hour costs of the Kinesis data stream. However, option C is incorrect because the amount of data would exceed the 1 MB/s quota of a single shard.

8) B, D – In option B, the use of an Amazon Simple Queue Service (Amazon SQS) queue will decouple the main application from calls to the affiliate. This change will protect the main application from the reduced capacity of the affiliate. Additionally, failed requests can automatically return to the queue. In option D, a decreased number of concurrent invocations will prevent the affiliate application from getting overwhelmed.

Although option A will reduce the load on the Amazon EC2 instances, this solution will not reduce the number of requests to the affiliate application. Although option C will allow the AWS Lambda function to wait longer for the external call to return, this solution will not reduce the load on the overwhelmed affiliate application. Option E is incorrect because an increase in memory will have no effect on the interaction between the Lambda function and the affiliate tracking system.

9) A, D, F – AWS App Runner is a fully managed service that developers can use to quickly deploy containerized web applications with images that are stored in an Amazon Elastic Container Registry (Amazon ECR) repository. Option A is correct because Cross-Region Replication makes a copy of the repository in a second AWS Region. Option D is correct because you can use Route 53 to host the custom domain name and to route traffic to resources in multiple AWS Regions. Option F is correct because Amazon Aurora global databases extend across multiple Regions and are designed for globally distributed applications.

Option B is incorrect because a VPC endpoint will not provide access to an image that is stored in a different Region. In option C, no such configuration exists in App Runner. Although option E would work, the introduction of Amazon DynamoDB would require more change to the architecture than the use of an Aurora global database. The question asks for the least change to the architecture.

10) B, C – In option B, by placing the web tier behind an Application Load Balancer (ALB), you can improve availability and scalability of the web tier. The ALB serves as the single point of contact for clients and distributes incoming application traffic to the Amazon EC2 instances. Option C is correct because Amazon Aurora Serverless provides high performance and high availability with reduced operational complexity.

Option A is incorrect because additional EC2 instances will not minimize operational overhead. A managed service would be a better option. Option D is incorrect because the application includes Windows instances, which are not available for Graviton2. Option E is incorrect because a company-managed load balancer will not minimize operational overhead.