SCS-C02^Q&As^

AWS Certified Security - Specialty

QUESTION 1

A company is planning to run a number of Admin related scripts using the IAM Lambda service. There is a need to understand if there are any errors encountered when the script run. How can this be accomplished in the most effective manner?

A. Use Cloudwatch metrics and logs to watch for errors

B. Use Cloudtrail to monitor for errors

C. Use the IAM Config service to monitor for errors

D. Use the IAM inspector service to monitor for errors

Correct Answer: A

The IAM Documentation mentions the following IAM Lambda automatically monitors Lambda functions on your behalf, reporting metrics through Amazon CloudWatch. To help you troubleshoot failures in a function. Lambda logs all requests handled by your function and also automatically stores logs generated by your code through Amazon CloudWatch Logs. Option B,C and D are all invalid because these services cannot be used to monitor for errors. I For more information on Monitoring Lambda functions, please visit the following URL: https://docs.IAM.amazon.com/lambda/latest/dg/monitorine-functions-loes.htmll The correct answer is: Use Cloudwatch metrics and logs to watch for errors Submit your Feedback/Queries to our Experts

QUESTION 2

A Development team has built an experimental environment to test a simple stale web application It has built an isolated VPC with a private and a public subnet. The public subnet holds only an Application Load Balancer a NAT gateway, and an internet gateway. The private subnet holds ail of the Amazon EC2 instances

There are 3 different types of servers Each server type has its own Security Group that limits access lo only required connectivity. The Security Groups nave both inbound and outbound rules applied Each subnet has both inbound and outbound network ACls applied to limit access to only required connectivity

Which of the following should the team check if a server cannot establish an outbound connection to the internet? (Select THREE.)

A. The route tables and the outbound rules on the appropriate private subnet security group

B. The outbound network ACL rules on the private subnet and the Inbound network ACL rules on the public subnet

C. The outbound network ACL rules on the private subnet and both the inbound and outbound rules on the public subnet

D. The rules on any host-based firewall that may be applied on the Amazon EC2 instances

E. The Security Group applied to the Application Load Balancer and NAT gateway

F. That the 0.0.0./0 route in the private subnet route table points to the internet gateway in the public subnet

Correct Answer: CEF

QUESTION 3

A Security Analyst attempted to troubleshoot the monitoring of suspicious security group changes. The Analyst was told that there is an Amazon CloudWatch alarm in place for these IAM CloudTrail log events. The Analyst tested the monitoring setup by making a configuration change to the security group but did not receive any alerts.

Which of the following troubleshooting steps should the Analyst perform?

A. Ensure that CloudTrail and S3 bucket access logging is enabled for the Analyst\\'s IAM account.

B. Verify that a metric filter was created and then mapped to an alarm. Check the alarm notification action.

C. Check the CloudWatch dashboards to ensure that there is a metric configured with an appropriate dimension for security group changes.

D. Verify that the Analyst\\'s account is mapped to an IAM policy that includes permissions for cloudwatch: GetMetricStatistics and Cloudwatch: ListMetrics.

Correct Answer: B

MetricFilter:

Type: \\'IAM::Logs::MetricFilter\\'

Properties:

LogGroupName: \\'\\'

FilterPattern: >{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName = AuthorizeSecurityGroupEgress) || ($.eventName =

RevokeSecurityGroupIngress) || ($.eventName = RevokeSecurityGroupEgress) || ($.eventName = CreateSecurityGroup) || ($.eventName = DeleteSecurityGroup) } MetricTransformations:

-MetricValue: \\'1\\' MetricNamespace: CloudTrailMetrics MetricName: SecurityGroupEventCount

QUESTION 4

A security administrator has enabled AWS Security Hub for all the AWS accounts in an organization in AWS Organizations. The security team wants near-real-time response and remediation for deployed AWS resources that do not meet

security standards. All changes must be centrally logged for auditing purposes.

The organization has reached the quotas for the number of SCPs attached to an OU and SCP document size. The team wants to avoid making any changes to any of the SCPs. The solution must maximize scalability and cost-effectiveness.

Which combination of actions should the security administrator take to meet these requirements? (Choose three.)

A. Create an AWS Config custom rule to detect configuration changes to AWS resources. Create an AWS Lambda function to remediate the AWS resources in the delegated administrator AWS account.

B. Use AWS Systems Manager Change Manager to track configuration changes to AWS resources. Create a Systems Manager document to remediate the AWS resources in the delegated administrator AWS account.

C. Create a Security Hub custom action to reference in an Amazon EventBridge event rule in the delegated administrator AWS account.

D. Create an Amazon EventBridge event rule to Invoke an AWS Lambda function that will take action on AWS resources.

E. Create an Amazon EventBridge event rule to invoke an AWS Lambda function that will evaluate AWS resource configuration for a set of API requests and create a finding for noncompllant AWS resources.

F. Create an Amazon EventBridge event rule to invoke an AWS Lambda function on a schedule to assess specific AWS Config rules.

Correct Answer: ACD

QUESTION 5

A security engineer is creating an AWS Lambda function. The Lambda function needs to use a role that is named LambdaAuditRole to assume a role that is named AcmeAuditFactoryRole in a different AWS account.

When the code is processed, the following error message appears: "An error oc-curred (AccessDenied) when calling the AssumeRole operation."

Which combination of steps should the security engineer take to resolve this er-ror? (Select TWO.)

A. Ensure that LambdaAuditRole has the sts:AssumeRole permission for Ac- meAuditFactoryRole.

B. Ensure that LambdaAuditRole has the AWSLambdaBasicExecutionRole managed policy attached.

C. Ensure that the trust policy for AcmeAuditFactoryRole allows the sts:AssumeRole action from LambdaAuditRole.

D. Ensure that the trust policy for LambdaAuditRole allows the sts:AssumeRole action from the lambda.amazonaws.com service.

E. Ensure that the sts:AssumeRole API call is being issued to the us-east-I Region endpoint.

Correct Answer: AC