

Amazon-Web-Services

Exam Questions SCS-C03

AWS Certified Security - Specialty



NEW QUESTION 1

AWS Config cannot deliver configuration snapshots to Amazon S3. Which TWO actions will remediate this issue?

- A. Verify the S3 bucket policy allows config.amazonaws.com.
- B. Verify the IAM role has s3:GetBucketAcl and s3:PutObject permissions.
- C. Verify the S3 bucket can assume the IAM role.
- D. Verify IAM policy allows AWS Config to write logs.
- E. Modify AWS Config API permissions.

Answer: AB

NEW QUESTION 2

A company uses AWS Organizations to manage an organization that consists of three workload OUs: Production, Development, and Testing. The company uses AWS CloudFormation templates to define and deploy workload infrastructure in AWS accounts that are associated with the OUs. Different SCPs are attached to each workload OU.

The company successfully deployed a CloudFormation stack update to workloads in the Development OU and the Testing OU. When the company uses the same CloudFormation template to deploy the stack update in an account in the Production OU, the update fails.

The error message reports insufficient IAM permissions.

What is the FIRST step that a security engineer should take to troubleshoot this issue?

- A. Review the AWS CloudTrail logs in the account in the Production O
- B. Search for any failed API calls from CloudFormation during the deployment attempt.
- C. Remove all the SCPs that are attached to the Production O
- D. Rerun the CloudFormation stack update to determine if the SCPs were preventing the CloudFormation API calls.
- E. Confirm that the role used by CloudFormation has sufficient permissions to create, update, and delete the resources that are referenced in the CloudFormation template.
- F. Make all the SCPs that are attached to the Production OU the same as the SCPs that are attached to the Testing OU.

Answer: A

NEW QUESTION 3

A company hosts its public website on Amazon EC2 instances behind an Application Load Balancer (ALB). The website is experiencing a global DDoS attack from a specific IoT device brand that uses a unique user agent. A security engineer is creating an AWS WAF web ACL and will associate it with the ALB.

Which rule statement will mitigate the current attack and future attacks from these IoT devices without blocking legitimate customers?

- A. Use an IP set match rule statement.
- B. Use a geographic match rule statement.
- C. Use a rate-based rule statement.
- D. Use a string match rule statement on the user agent.

Answer: D

NEW QUESTION 4

A company's security team wants to receive near-real-time email notifications about AWS abuse reports related to DoS attacks. An Amazon SNS topic already exists and is subscribed to by the security team.

What should the security engineer do next?

- A. Poll Trusted Advisor for abuse notifications by using a Lambda function.
- B. Create an Amazon EventBridge rule that matches AWS Health events for AWS_ABUSE_DOS_REPORT and publishes to SNS.
- C. Poll the AWS Support API for abuse cases by using a Lambda function.
- D. Detect abuse reports by using CloudTrail logs and CloudWatch alarms.

Answer: B

NEW QUESTION 5

A company's security engineer receives an abuse notification from AWS indicating that malware is being hosted from the company's AWS account. The security engineer discovers that an IAM user created a new Amazon S3 bucket without authorization.

Which combination of steps should the security engineer take to MINIMIZE the consequences of this compromise? (Select THREE.)

- A. Encrypt all AWS CloudTrail logs.
- B. Turn on Amazon GuardDuty.
- C. Change the password for all IAM users.
- D. Rotate or delete all AWS access keys.
- E. Take snapshots of all Amazon Elastic Block Store (Amazon EBS) volumes.
- F. Delete any resources that are unrecognized or unauthorized.

Answer: BDF

NEW QUESTION 6

A security engineer wants to forward custom application-security logs from an Amazon EC2 instance to Amazon CloudWatch. The security engineer installs the CloudWatch agent on the EC2 instance and adds the path of the logs to the CloudWatch configuration file.

However, CloudWatch does not receive the logs. The security engineer verifies that the awslogs service is running on the EC2 instance.

What should the security engineer do next to resolve the issue?

- A. Add AWS CloudTrail to the trust policy of the EC2 instanc
- B. Send the custom logs to CloudTrail instead of CloudWatch.

- C. Add Amazon S3 to the trust policy of the EC2 instance
- D. Configure the application to write the custom logs to an S3 bucket that CloudWatch can use to ingest the logs.
- E. Add Amazon Inspector to the trust policy of the EC2 instance
- F. Use Amazon Inspector instead of the CloudWatch agent to collect the custom logs.
- G. Attach the CloudWatchAgentServerPolicy AWS managed policy to the EC2 instance role.

Answer: D

NEW QUESTION 7

A company wants to establish separate AWS Key Management Service (AWS KMS) keys to use for different AWS services. The company's security engineer created a key policy to allow the infrastructure deployment team to create encrypted Amazon Elastic Block Store (Amazon EBS) volumes by assuming the InfrastructureDeployment IAM role. The security engineer recently discovered that IAM roles other than the InfrastructureDeployment role used this key for other services.

Which change to the policy should the security engineer make to resolve these issues?

- A. In the statement block that contains the Sid "Allow use of the key", under the "Condition" block, change StringEquals to StringLike.
- B. In the policy document, remove the statement block that contains the Sid "Enable IAM User Permissions". Add key management policies to the KMS policy.
- C. In the statement block that contains the Sid "Allow use of the key", under the "Condition" block, change the kms:ViaService value to ec2.us-east-1.amazonaws.com.
- D. In the policy document, add a new statement block that grants the kms:Disable* permission to the security engineer's IAM role.

Answer: C

NEW QUESTION 8

A company needs to build a code-signing solution using an AWS KMS asymmetric key and must store immutable evidence of key creation and usage for compliance and audit purposes.

Which solution meets these requirements?

- A. Create an Amazon S3 bucket with S3 Object Lock enable
- B. Create an AWS CloudTrail trail with log file validation enabled for KMS event
- C. Store logs in the bucket and grant auditors access.
- D. Log application events to Amazon CloudWatch Logs and export them.
- E. Capture KMS API calls using EventBridge and store them in DynamoDB.
- F. Track KMS usage with CloudWatch metrics and dashboards.

Answer: A

NEW QUESTION 9

A company has several Amazon S3 buckets that do not enforce encryption in transit. A security engineer must implement a solution that enforces encryption in transit for all the company's existing and future S3 buckets.

Which solution will meet these requirements?

- A. Enable AWS Config
- B. Create a proactive AWS Config Custom Policy rule
- C. Create a Guard clause to evaluate the S3 bucket policies to check for a value of True for the aws:SecureTransport condition key
- D. If the AWS Config rule evaluates to NON_COMPLIANT, block resource creation.
- E. Enable AWS Config
- F. Configure the s3-bucket-ssl-requests-only AWS Config managed rule and set the rule trigger type to Hybrid
- G. Create an AWS Systems Manager Automation runbook that applies a bucket policy to deny requests when the value of the aws:SecureTransport condition key is False
- H. Configure automatic remediation
- I. Set the runbook as the target of the rule.
- J. Enable Amazon Inspector
- K. Create a custom AWS Lambda rule
- L. Create a Lambda function that applies a bucket policy to deny requests when the value of the aws:SecureTransport condition key is False
- M. Set the Lambda function as the target of the rule.
- N. Create an AWS CloudTrail trail
- O. Enable S3 data events on the trail
- P. Create an AWS Lambda function that applies a bucket policy to deny requests when the value of the aws:SecureTransport condition key is False
- Q. Configure the CloudTrail trail to invoke the Lambda function.

Answer: B

NEW QUESTION 10

A company requires a specific software application to be installed on all new and existing Amazon EC2 instances across an AWS Organization. SSM Agent is installed and active.

How can the company continuously monitor deployment status of the software application?

- A. Use AWS Config organization-wide with the ec2-managedinstance-applications-required managed rule and specify the application name.
- B. Use approved AMIs rule organization-wide.
- C. Use Distributor package and review output.
- D. Use Systems Manager Application Manager inventory filtering.

Answer: A

NEW QUESTION 10

A company has a PHP-based web application that uses Amazon S3 as an object store for user files. The S3 bucket is configured for server-side encryption with Amazon S3 managed keys (SSE-S3). New requirements mandate full control of encryption keys.

Which combination of steps must a security engineer take to meet these requirements? (Select THREE.)

- A. Create a new customer managed key in AWS Key Management Service (AWS KMS).
- B. Change the SSE-S3 configuration on the S3 bucket to server-side encryption with customer-provided keys (SSE-C).
- C. Configure the PHP SDK to use the SSE-S3 key before upload.
- D. Create an AWS managed key for Amazon S3 in AWS KMS.
- E. Change the SSE-S3 configuration on the S3 bucket to server-side encryption with AWS KMS managed keys (SSE-KMS).
- F. Change all the S3 objects in the bucket to use the new encryption key.

Answer: AEF

NEW QUESTION 11

A company is using AWS Organizations with nested OUs to manage AWS accounts. The company has a custom compliance monitoring service for the accounts. The monitoring service runs as an AWS Lambda function and is invoked by Amazon EventBridge Scheduler. The company needs to deploy the monitoring service in all existing and future accounts in the organization. The company must avoid using the organization's management account when the management account is not required. Which solution will meet these requirements?

- A. Create a CloudFormation stack set in the organization's management account and manually add new accounts.
- B. Configure a delegated administrator account for AWS CloudFormation.
- C. Create a CloudFormation StackSet in the delegated administrator account targeting the organization root with automatic deployment enabled.
- D. Use Systems Manager delegated administration and Automation to deploy the Lambda function and schedule.
- E. Create a Systems Manager Automation runbook in the management account and share it to accounts.

Answer: B

NEW QUESTION 16

A company has AWS accounts in an organization in AWS Organizations. An Amazon S3 bucket in one account is publicly accessible. A security engineer must remove public access and ensure the bucket cannot be made public again. Which solution will meet these requirements?

- A. Enforce KMS encryption and deny s3:GetObject by SCP.
- B. Enable PublicAccessBlock and deny s3:GetObject by SCP.
- C. Enable PublicAccessBlock and deny s3:PutPublicAccessBlock by SCP.
- D. Enable Object Lock governance and deny s3:PutPublicAccessBlock by SCP.

Answer: C

NEW QUESTION 18

A company is implementing new compliance requirements to meet customer needs. According to the new requirements, the company must not use any Amazon RDS DB instances or DB clusters that lack encryption of the underlying storage. The company needs a solution that will generate an email alert when an unencrypted DB instance or DB cluster is created. The solution also must terminate the unencrypted DB instance or DB cluster. Which solution will meet these requirements in the MOST operationally efficient manner?

- A. Create an AWS Config managed rule to detect unencrypted RDS storage.
- B. Configure an automatic remediation action to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic that includes an AWS Lambda function and an email delivery target as subscriber.
- C. Configure the Lambda function to delete the unencrypted resource.
- D. Create an AWS Config managed rule to detect unencrypted RDS storage.
- E. Configure a manual remediation action to invoke an AWS Lambda function.
- F. Configure the Lambda function to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic and to delete the unencrypted resource.
- G. Create an Amazon EventBridge rule that evaluates RDS event patterns and is initiated by the creation of DB instances or DB cluster.
- H. Configure the rule to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic that includes an AWS Lambda function and an email delivery target as subscriber.
- I. Configure the Lambda function to delete the unencrypted resource.
- J. Create an Amazon EventBridge rule that evaluates RDS event patterns and is initiated by the creation of DB instances or DB cluster.
- K. Configure the rule to invoke an AWS Lambda function.
- L. Configure the Lambda function to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic and to delete the unencrypted resource.

Answer: A

NEW QUESTION 19

Notify when IAM roles are modified.

- A. Use Amazon Detective.
- B. Use EventBridge with CloudTrail events.
- C. Use CloudWatch metric filters.
- D. Use CloudWatch subscription filters.

Answer: B

NEW QUESTION 23

A company recently experienced a malicious attack on its cloud-based environment. The company successfully contained and eradicated the attack. A security engineer is performing incident response work. The security engineer needs to recover an Amazon RDS database cluster to the last known good version. The database cluster is configured to generate automated backups with a retention period of 14 days. The initial attack occurred 5 days ago at exactly 3:15 PM. Which solution will meet this requirement?

- A. Identify the Regional cluster ARN for the database.

- B. Use the ARN to restore the Regional cluster by using the restore to point in time featur
- C. Set a target time 5 days ago at 3:14 PM.
- D. Identify the Regional cluster ARN for the databas
- E. List snapshots that have been taken of the cluste
- F. Restore the database by using the snapshot that has a creation time that is closest to 5 days ago at 3:14 PM.
- G. List all snapshots that have been taken of all the company's RDS database
- H. Identify the snapshot that was taken closest to 5 days ago at 3:14 PM and restore it.
- I. Identify the Regional cluster ARN for the databas
- J. Use the ARN to restore the Regional cluster by using the restore to point in time featur
- K. Set a target time 14 days ago.

Answer: A

NEW QUESTION 26

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SCS-C03 Practice Exam Features:

- * SCS-C03 Questions and Answers Updated Frequently
- * SCS-C03 Practice Questions Verified by Expert Senior Certified Staff
- * SCS-C03 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SCS-C03 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SCS-C03 Practice Test Here](#)