Amazon-Web-Services

Exam Questions SCS-C03

AWS Certified Security - Specialty

NEW QUESTION 1
A security team manages a company??s AWS Key Management Service (AWS KMS) customer managed keys. Only members of the security team can administer the KMS keys. The company's application team has a software process that needs temporary access to the keys occasionally. The security team needs to provide the application team's software process with access to the keys.
Which solution will meet these requirements with the LEAST operational overhead?

A. Export the KMS key material to an on-premises hardware security module (HSM). Give the application team access to the key material.
B. Edit the key policy that grants the security team access to the KMS keys by adding the application team as principal
C. Revert this change when the application team no longer needs access.
D. Create a key grant to allow the application team to use the KMS key
E. Revoke the grant when the application team no longer needs access.
F. Create a new KMS key by generating key material on premise
G. Import the key material to AWS KMS whenever the application team needs acces
H. Grant the application team permissions to use the key.

Answer: C

NEW QUESTION 2
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 3
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 instanc
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 instanc
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 4
A company has a VPC that has no internet access and has the private DNS hostnames option enabled. An Amazon Aurora database is running inside the VPC. A security engineer wants to use AWS Secrets Manager to automatically rotate the credentials for the Aurora database. The security engineer configures the Secrets Manager default AWS Lambda rotation function to run inside the same VPC that the Aurora database uses. However, the security engineer determines that the password cannot be rotated properly because the Lambda function cannot communicate with the Secrets Manager endpoint.
What is the MOST secure way that the security engineer can give the Lambda function the ability to communicate with the Secrets Manager endpoint?

A. Add a NAT gateway to the VPC to allow access to the Secrets Manager endpoint.
B. Add a gateway VPC endpoint to the VPC to allow access to the Secrets Manager endpoint.
C. Add an interface VPC endpoint to the VPC to allow access to the Secrets Manager endpoint.
D. Add an internet gateway for the VPC to allow access to the Secrets Manager endpoint.

Answer: C

NEW QUESTION 5
A company is building a secure solution that relies on an AWS Key Management Service (AWS KMS) customer managed key. The company wants to allow AWS Lambda to use the KMS key. However, the company wants to prevent Amazon EC2 from using the key.
Which solution will meet these requirements?

A. Use IAM explicit deny for EC2 instance profiles and allow for Lambda roles.
B. Use a KMS key policy with kms:ViaService conditions to allow Lambda usage and deny EC2 usage.
C. Use aws:SourceIp and aws:AuthorizedService condition keys in the KMS key policy.
D. Use an SCP to deny EC2 and allow Lambda.

Answer: B

NEW QUESTION 6
A security administrator is setting up a new AWS account. The security administrator wants to secure the data that a company stores in an Amazon S3 bucket. The security administrator also wants to reduce the chance of unintended data exposure and the potential for misconfiguration of objects that are in the S3 bucket.
Which solution will meet these requirements with the LEAST operational overhead?

A. Configure the S3 Block Public Access feature for the AWS account.
B. Configure the S3 Block Public Access feature for all objects that are in the bucket.
C. Deactivate ACLs for objects that are in the bucket.
D. Use AWS PrivateLink for Amazon S3 to access the bucket.

Answer: A

NEW QUESTION 7
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 8
A company has an encrypted Amazon Aurora DB cluster in the us-east-1 Region that uses an AWS KMS customer managed key. The company must copy a DB snapshot to the us- west-1 Region but cannot access the encryption key across Regions.
What should the company do to properly encrypt the snapshot in us-west-1?

A. Store the customer managed key in AWS Secrets Manager in us-west-1.
B. Create a new customer managed key in us-west-1 and use it to encrypt the snapshot.
C. Create an IAM policy to allow access to the key in us-east-1 from us-west-1.
D. Create an IAM policy that allows RDS in us-west-1 to access the key in us-east-1.

Answer: B

NEW QUESTION 9
A company??s data scientists use Amazon SageMaker with datasets stored in Amazon S3. Data older than 45 days must be removed according to policy.
Which action should enforce this policy?

A. Configure an S3 Lifecycle rule to delete objects after 45 days.
B. Create a Lambda function triggered on object upload to delete old data.
C. Create a scheduled Lambda function to delete old objects monthly.
D. Configure S3 Intelligent-Tiering.

Answer: A

NEW QUESTION 10
A security engineer needs to prepare Amazon EC2 instances for quarantine during a security incident. AWS Systems Manager Agent (SSM Agent) is installed, and a script exists to install and update forensic tools.
Which solution will quarantine EC2 instances during a security incident?

A. Track SSM Agent versions with AWS Config.
B. Configure Session Manager to deny external connections.
C. Store the script in Amazon S3 and grant read access.
D. Configure IAM permissions for the SSM Agent to run the script as a Systems Manager Run Command document.

Answer: D

NEW QUESTION 10
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 Confi
B. Create a proactive AWS Config Custom Policy rul
C. Create aGuard clause to evaluate the S3 bucket policies to check for a value of True for the aws:SecureTransport condition ke
D. If the AWS Config rule evaluates to NON_COMPLIANT, block resource creation.
E. Enable AWS Confi
F. Configure the s3-bucket-ssl-requests-only AWS Config managed rule and set the rule trigger type to Hybri
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 Fals
H. Configure automatic remediatio
I. Set the runbook as the target of the rule.
J. Enable Amazon Inspecto
K. Create a custom AWS Lambda rul
L. Create a Lambda function that applies a bucket policy to deny requests when the value of the aws:SecureTransport condition key is Fals
M. Set the Lambda function as the target of the rule.
N. Create an AWS CloudTrail trai
O. Enable S3 data events on the trai
P. Create an AWS Lambda function that applies a bucket policy to deny requests when the value of the aws:SecureTransport condition key is Fals

Q. Configure the CloudTrail trail to invoke the Lambda function.

Answer: B

NEW QUESTION 15
A security engineer discovers that a company's user passwords have no required minimum length. The company uses the following identity providers (IdPs):
• AWS Identity and Access Management (IAM) federated with on-premises Active Directory
• Amazon Cognito user pools that contain the user database for an AWS Cloud application Which combination of actions should the security engineer take to implement a required minimum password length? (Select TWO.)

A. Update the password length policy in the IAM configuration.
B. Update the password length policy in the Amazon Cognito configuration.
C. Update the password length policy in the on-premises Active Directory configuration.
D. Create an SCP in AWS Organizations to enforce minimum password length.
E. Create an IAM policy with a minimum password length condition.

Answer: BC

NEW QUESTION 16
A company??s web application runs on Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group. An AWS WAF web ACL is associated with the ALB. Instance logs are lost after reboots. The operations team suspects malicious activity targeting a specific PHP file.
Which set of actions will identify the suspect attacker??s IP address for future occurrences?

A. Configure VPC Flow Logs and search for PHP file activity.
B. Install the CloudWatch agent on the ALB and export application logs.
C. Export ALB access logs to Amazon OpenSearch Service and search them.
D. Configure the web ACL to send logs to Amazon Kinesis Data Firehos
E. Deliver logs to Amazon S3 and query them with Amazon Athena.

Answer: D

NEW QUESTION 19
A company runs a web application on a fleet of Amazon EC2 instances in an Auto Scaling group. Amazon GuardDuty and AWS Security Hub are enabled. The security engineer needs an automated response to anomalous traffic that follows AWS best practices and minimizes application disruption.
Which solution will meet these requirements?

A. Use EventBridge to disable the instance profile access keys.
B. Use EventBridge to invoke a Lambda function that removes the affected instance from the Auto Scaling group and isolates it with a restricted security group.
C. Use Security Hub to update the subnet network ACL to block traffic.
D. Send GuardDuty findings to Amazon SNS for email notification.

Answer: B

NEW QUESTION 20
A company is running an application in the eu-west-1 Region. The application uses an AWS Key Management Service (AWS KMS) customer managed key to encrypt sensitive data. The company plans to deploy the application in the eu-north-1 Region. A security engineer needs to implement a key management solution for the application deployment in the new Region. The security engineer must minimize changes to the application code.
Which change should the security engineer make to the AWS KMS configuration to meet these requirements?

A. Update the key policies in eu-west-1. Point the application in eu-north-1 to use the same customer managed key as the application in eu-west-1.
B. Allocate a new customer managed key to eu-north-1 to be used by the application that is deployed in that Region.
C. Allocate a new customer managed key to eu-north-1. Create the same alias name for both key
D. Configure the application deployment to use the key alias.
E. Allocate a new customer managed key to eu-north-1. Create an alias for eu--1. Change the application code to point to the alias for eu--1.

Answer: C

NEW QUESTION 22
A company stores infrastructure and application code in web-based, third-party, Git- compatible code repositories outside of AWS. The company wants to give the code repositories the ability to securely authenticate and assume an existing IAM role within the company's AWS account by using OpenID Connect (OIDC).
Which solution will meet these requirements?

A. Create an OIDC identity provider (IdP) by using AWS Identity and Access Management (IAM) federatio
B. Modify the trust policy of the IAM role to allow the code repositories to assume the IAM role.
C. Use AWS Identity and Access Management (IAM) Roles Anywhere to create a trust anchor that uses OID
D. Modify the trust policy of the IAM role to allow the code repositories to assume the IAM role.
E. Set up an account instance of AWS IAM Identity Cente
F. Configure access to the code repositories as a customer managed OIDC applicatio
G. Grant the application access to the IAM role.
H. Use AWS Resource Access Manager (AWS RAM) to create a new resource share that uses OID
I. Limit the resource share to the specified code repositorie
J. Grant the IAM role access to the resource share.

Answer: A

NEW QUESTION 26
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 30
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 andmanually add new accounts.
B. Configure a delegated administrator account for AWS CloudFormatio
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 35
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 39
A company needs centralized log monitoring with automatic detection across hundreds of AWS accounts.
Which solution meets these requirements with the LEAST operational effort?

A. Designate a GuardDuty administrator account and enable protections.
B. Centralize CloudWatch logs and use Inspector.
C. Centralize CloudTrail logs and query with Athena.
D. Stream logs to Kinesis and process with Lambda.

Answer: A

NEW QUESTION 43
A company runs a global ecommerce website using Amazon CloudFront. The company must block traffic from specific countries to comply with data regulations.
Which solution will meet these requirements MOST cost-effectively?

A. Use AWS WAF IP match rules.
B. Use AWS WAF geo match rules.
C. Use CloudFront geo restriction to deny the countries.
D. Use geolocation headers in CloudFront.

Answer: C

NEW QUESTION 45
A company sends Apache logs from EC2 Auto Scaling instances to a CloudWatch Logs log group with 1-year retention. A suspicious IP address appears in logs. A security engineer needs to analyze the past week of logs to count requests from that IP and list requested URLs.
What should the engineer do with the LEAST effort?

A. Export to S3 and use Macie.
B. Stream to OpenSearch and analyze.
C. Use CloudWatch Logs Insights with queries.
D. Export to S3 and use AWS Glue.

Answer: C

NEW QUESTION 49
A security engineer needs to implement a solution to identify any sensitive data that is stored in an Amazon S3 bucket. The solution must report on sensitive data in the S3 bucket by using an existing Amazon Simple Notification Service (Amazon SNS) topic.
Which solution will meet these requirements with the LEAST implementation effort?

A. Enable AWS Confi
B. Configure AWS Config to monitor for sensitive data in the S3 bucket and to send notifications to the SNS topic.
C. Create an AWS Lambda function to scan the S3 bucket for sensitive data that matches a patter
D. Program the Lambda function to send notifications to the SNS topic.
E. Configure Amazon Macie to use managed data identifiers to identify and categorize sensitive dat
F. Create an Amazon EventBridge rule to send notifications to the SNS topic.
G. Enable Amazon GuardDut
H. Configure AWS CloudTrail S3 data event
I. Create an Amazon CloudWatch alarm that reacts to GuardDuty findings and sends notifications to the SNS topic.

Answer: C

NEW QUESTION 51
A company that uses AWS Organizations is using AWS IAM Identity Center to administer access to AWS accounts. A security engineer is creating a custom permission set in IAM Identity Center. The company will use the permission set across multiple accounts. An AWS managed policy and a customer managed policy are attached to the permission set. The security engineer has full administrative permissions and is operating in the management account.
When the security engineer attempts to assign the permission set to an IAM Identity Center user who has access to multiple accounts, the assignment fails.
What should the security engineer do to resolve this failure?

A. Create the customer managed policy in every account where the permission set is assigne
B. Give the customer managed policy the same name and same permissions in each account.
C. Remove either the AWS managed policy or the customer managed policy from the permission se
D. Create a second permission set that includes the removed polic
E. Apply the permission sets separately to the user.
F. Evaluate the logic of the AWS managed policy and the customer managed polic
G. Resolve any policy conflicts in the permission set before deployment.
H. Do not add the new permission set to the use
I. Instead, edit the user's existing permission set to include the AWS managed policy and the customer managed policy.

Answer: A

NEW QUESTION 56
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 databas
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 60
A security engineer needs to control access to data that is encrypted with an AWS Key Management Service (AWS KMS) customer managed key. The security engineer also needs to use additional authenticated data (AAD) to prevent tampering with ciphertext.
Which solution will meet these requirements?

A. Pass the key alias to AWS KMS when calling the Encrypt and Decrypt API actions.
B. Use IAM policies to restrict access to the Encrypt and Decrypt API actions.
C. Use the kms:EncryptionContext condition key when defining IAM policies for the customer managed key.
D. Use key policies to restrict access to the appropriate IAM groups.

Answer: C

NEW QUESTION 61
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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