

Exam Questions SCS-C03

AWS Certified Security - Specialty

<https://www.2passeasy.com/dumps/SCS-C03/>



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 has a web application that reads from and writes to an Amazon S3 bucket. The company needs to use AWS credentials to authenticate all S3 API calls to the S3 bucket. Which solution will provide the application with AWS credentials to make S3 API calls?

- A. Integrate with Cognito identity pools and use GetId to obtain AWS credentials.
- B. Integrate with Cognito identity pools and use AssumeRoleWithWebIdentity to obtain AWS credentials.
- C. Integrate with Cognito user pools and use the ID token to obtain AWS credentials.
- D. Integrate with Cognito user pools and use the access token to obtain AWS credentials.

Answer: B

NEW QUESTION 3

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 4

A company is attempting to conduct forensic analysis on an Amazon EC2 instance, but the company is unable to connect to the instance by using AWS Systems Manager Session Manager. The company has installed AWS Systems Manager Agent (SSM Agent) on the EC2 instance. The EC2 instance is in a subnet in a VPC that does not have an internet gateway attached. The company has associated a security group with the EC2 instance. The security group does not have inbound or outbound rules. The subnet's network ACL allows all inbound and outbound traffic. Which combination of actions will allow the company to conduct forensic analysis on the EC2 instance without compromising forensic data? (Select THREE.)

- A. Update the EC2 instance security group to add a rule that allows outbound traffic on port 443 for 0.0.0.0/0.
- B. Update the EC2 instance security group to add a rule that allows inbound traffic on port 443 to the VPC's CIDR range.
- C. Create an EC2 key pair
- D. Associate the key pair with the EC2 instance.
- E. Create a VPC interface endpoint for Systems Manager in the VPC where the EC2 instance is located.
- F. Attach a security group to the VPC interface endpoint
- G. Allow inbound traffic on port 443 to the VPC's CIDR range.
- H. Create a VPC interface endpoint for the EC2 instance in the VPC where the EC2 instance is located.

Answer: ADE

NEW QUESTION 5

A company runs an application on an Amazon EC2 instance. The application generates invoices and stores them in an Amazon S3 bucket. The instance profile that is attached to the instance has appropriate access to the S3 bucket. The company needs to share each invoice with multiple clients that do not have AWS credentials. Each client must be able to download only the client's own invoices. Clients must download their invoices within 1 hour of invoice creation. Clients must use only temporary credentials to access the company's AWS resources. Which additional step will meet these requirements?

- A. Update the S3 bucket policy to ensure that clients that use pre-signed URLs have the S3:Get* permission and the S3:List* permission to access S3 objects in the bucket.
- B. Add a StringEquals condition to the IAM role policy for the EC2 instance profile
- C. Configure the policy condition to restrict access based on the s3:ResourceTag/ClientId tag of each invoice
- D. Tag each generated invoice with the ID of its corresponding client.
- E. Update the script to use AWS Security Token Service (AWS STS) to obtain new credentials each time the script runs by assuming a new role that has S3:GetObject permission
- F. Use the credentials to generate the pre-signed URLs.
- G. Generate an access key and a secret key for an IAM user that has S3:GetObject permissions on the S3 bucket
- H. Embed the keys into the script
- I. Use the keys to generate the pre-signed URLs.

Answer: B

NEW QUESTION 6

A security engineer has designed a VPC to segment private traffic from public traffic. The VPC includes two Availability Zones. Each Availability Zone contains one public subnet and one private subnet. Three route tables exist: one for the public subnets and one for each private subnet.

The security engineer discovers that all four subnets are routing traffic through the internet gateway that is attached to the VPC. Which combination of steps should the security engineer take to remediate this scenario? (Select TWO.)

- A. Verify that a NAT gateway has been provisioned in the public subnet in each Availability Zone.
- B. Verify that a NAT gateway has been provisioned in the private subnet in each Availability Zone.
- C. Modify the route tables for the public subnets to add a local route to the VPC CIDR range.
- D. Modify the route tables for the private subnets to route 0.0.0.0/0 to the NAT gateway in the public subnet of the same Availability Zone.
- E. Modify the route tables for the private subnets to route 0.0.0.0/0 to the internet gateway.

Answer: AD

NEW QUESTION 7

A company is running its application on AWS. The company has a multi-environment setup, and each environment is isolated in a separate AWS account. The company has an organization in AWS Organizations to manage the accounts. There is a single dedicated security account for the organization. The company must create an inventory of all sensitive data that is stored in Amazon S3 buckets across the organization's accounts. The findings must be visible from a single location. Which solution will meet these requirements?

- A. Set the security account as the delegated administrator for Amazon Macie and AWS Security Hub
- B. Enable and configure Macie to publish sensitive data findings to Security Hub.
- C. Set the security account as the delegated administrator for AWS Security Hub
- D. In each account, configure Amazon Inspector to scan the S3 buckets for sensitive data
- E. Publish sensitive data findings to Security Hub.
- F. In each account, configure Amazon Inspector to scan the S3 buckets for sensitive data
- G. Enable Amazon Inspector integration with AWS Trusted Advisor
- H. Publish sensitive data findings to Trusted Advisor.
- I. In each account, enable and configure Amazon Macie to detect sensitive data
- J. Enable Macie integration with AWS Trusted Advisor
- K. Publish sensitive data findings to Trusted Advisor.

Answer: A

NEW QUESTION 8

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 9

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 10

A company uses an organization in AWS Organizations to manage multiple AWS accounts. The company wants to centrally give users the ability to access Amazon Q Developer. Which solution will meet this requirement?

- A. Enable AWS IAM Identity Center and set up Amazon Q Developer as an AWS managed application.
- B. Enable Amazon Cognito and create a new identity pool for Amazon Q Developer.
- C. Enable Amazon Cognito and set up Amazon Q Developer as an AWS managed application.
- D. Enable AWS IAM Identity Center and create a new identity pool for Amazon Q Developer.

Answer: A

NEW QUESTION 10

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 12

A company runs an internet-accessible application on several Amazon EC2 instances that run Windows Server. The company used an instance profile to configure the EC2 instances. A security team currently accesses the VPC that hosts the EC2 instances by using an AWS Site-to-Site VPN tunnel from an on-premises office. The security team issues a policy that requires all external access to the VPC to be blocked in the event of a security incident. However, during an incident, the security team must be able to access the EC2 instances to obtain forensic information on the instances. Which solution will meet these requirements?

- A. Install EC2 Instance Connect on the EC2 instance
- B. Update the IAM policy for the IAM role to grant the required permission
- C. Use the AWS CLI to open a tunnel to connect to the instances.
- D. Install EC2 Instance Connect on the EC2 instance
- E. Configure the instances to permit access to the ec2-instance-connect command use
- F. Use the AWS Management Console to connect to the EC2 instances.
- G. Create an EC2 Instance Connect endpoint in the VP
- H. Configure an appropriate security group to allow access between the EC2 instances and the endpoint
- I. Use the AWS CLI to open a tunnel to connect to the instances.
- J. Create an EC2 Instance Connect endpoint in the VP
- K. Configure an appropriate security group to allow access between the EC2 instances and the endpoint
- L. Use the AWS Management Console to connect to the EC2 instances.

Answer: D

NEW QUESTION 13

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 18

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 19

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 24

A company uses AWS to run a web application that manages ticket sales in several countries. The company recently migrated the application to an architecture that includes Amazon API Gateway, AWS Lambda, and Amazon Aurora Serverless. The company needs the application to comply with Payment Card Industry Data Security Standard (PCI DSS) v4.0. A security engineer must generate a report that shows the effectiveness of the PCI DSS v4.0 controls that apply to the

application. The company's compliance team must be able to add manual evidence to the report. Which solution will meet these requirements?

- A. Enable AWS Trusted Adviso
- B. Configure all the Trusted Advisor check
- C. Manually map the checks against the PCI DSS v4.0 standard to generate the report.
- D. Enable and configure AWS Confi
- E. Deploy the Operational Best Practices for PCI DSS conformance pack in AWS Confi
- F. Use AWS Config to generate the report.
- G. Enable AWS Security Hu
- H. Enable the Security Hub PCI DSS security standar
- I. Use the AWS Management Console to download the report from the security standard.
- J. Create an AWS Audit Manager assessment that uses the AWS managed PCI DSS v4.0 standard framewor
- K. Add all evidence to the assessmen
- L. Generate the report in Audit Manager for download.

Answer: D

NEW QUESTION 27

A company is planning to deploy a new log analysis environment. The company needs to analyze logs from multiple AWS services in near real time. The solution must provide the ability to search the logs and must send alerts to an existing Amazon Simple Notification Service (Amazon SNS) topic when specific logs match detection rules. Which solution will meet these requirements?

- A. Analyze the logs by using Amazon OpenSearch Servic
- B. Search the logs from the OpenSearch AP
- C. Use OpenSearch Service Security Analytics to match logs with detection rules and to send alerts to the SNS topic.
- D. Analyze the logs by using AWS Security Hu
- E. Search the logs from the Findings page in Security Hu
- F. Create custom actions to match logs with detection rules and to send alerts to the SNS topic.
- G. Analyze the logs by using Amazon CloudWatch Log
- H. Use a subscription filter to match logs with detection rules and to send alerts to the SNS topi
- I. Search the logs manually by using CloudWatch Logs Insights.
- J. Analyze the logs by using Amazon QuickSigh
- K. Search the logs by listing the query results in a dashboar
- L. Run queries to match logs with detection rules and to send alerts to the SNS topic.

Answer: A

NEW QUESTION 28

CloudFormation stack deployments fail for some users due to permission inconsistencies. Which combination of steps will ensure consistent deployments MOST securely? (Select THREE.)

- A. Create a composite principal service role.
- B. Create a service role with cloudformation.amazonaws.com as the principal.
- C. Attach scoped policies to the service role.
- D. Attach service ARNs in policy resources.
- E. Update each stack to use the service role.
- F. Allow iam:PassRole to the service role.

Answer: BEF

NEW QUESTION 30

A company's security engineer receives an alert that indicates that an unexpected principal is accessing a company-owned Amazon Simple Queue Service (Amazon SQS) queue. All the company's accounts are within an organization in AWS Organizations. The security engineer must implement a mitigation solution that minimizes compliance violations and investment in tools outside of AWS. What should the security engineer do to meet these requirements?

- A. Create security groups and attach them to all SQS queues.
- B. Modify network ACLs in all VPCs to restrict inbound traffic.
- C. Create interface VPC endpoints for Amazon SQ
- D. Restrict access using aws:SourceVpce and aws:PrincipalOrgId conditions.
- E. Use a third-party cloud access security broker (CASB).

Answer: C

NEW QUESTION 34

A company has an AWS account that hosts a production application. The company receives an email notification that Amazon GuardDuty has detected an Impact:IAMUser/AnomalousBehavior finding in the account. A security engineer needs to run the investigation playbook for this security incident and must collect and analyze the information without affecting the application. Which solution will meet these requirements MOST quickly?

- A. Log in to the AWS account by using read-only credential
- B. Review the GuardDuty finding for details about the IAM credentials that were use
- C. Use the IAM console to add a DenyAll policy to the IAM principal.
- D. Log in to the AWS account by using read-only credential
- E. Review the GuardDuty finding to determine which API calls initiated the findin
- F. Use Amazon Detective to review the API calls in context.
- G. Log in to the AWS account by using administrator credential
- H. Review the GuardDuty finding for details about the IAM credentials that were use

- I. Use the IAM console to add a DenyAll policy to the IAM principal.
- J. Log in to the AWS account by using read-only credential
- K. Review the GuardDuty finding to determine which API calls initiated the findin
- L. Use AWS CloudTrail Insights and AWS CloudTrail Lake to review the API calls in context.

Answer: B

NEW QUESTION 39

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 AMLs rule organization-wide.
- C. Use Distributor package and review output.
- D. Use Systems Manager Application Manager inventory filtering.

Answer: A

NEW QUESTION 44

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 46

A company detects bot activity targeting Amazon Cognito user pool endpoints. The solution must block malicious requests while maintaining access for legitimate users.

Which solution meets these requirements?

- A. Enable Amazon Cognito threat protection.
- B. Restrict access to authenticated users only.
- C. Associate AWS WAF with the Cognito user pool.
- D. Monitor requests with CloudWatch.

Answer: A

NEW QUESTION 47

A company is planning to migrate its applications to AWS in a single AWS Region. The company??s applications will use a combination of Amazon EC2 instances, Elastic Load Balancing (ELB) load balancers, and Amazon S3 buckets. The company wants to complete the migration as quickly as possible. All the applications must meet the following requirements:

- Data must be encrypted at rest.
- Data must be encrypted in transit.
- Endpoints must be monitored for anomalous network traffic.

Which combination of steps should a security engineer take to meet these requirements with the LEAST effort? (Select THREE.)

- A. Install the Amazon Inspector agent on EC2 instances by using AWS Systems Manager Automation.
- B. Enable Amazon GuardDuty in all AWS accounts.
- C. Create VPC endpoints for Amazon EC2 and Amazon S3. Update VPC route tables to use only the secure VPC endpoints.
- D. Configure AWS Certificate Manager (ACM). Configure the load balancers to use certificates from ACM.
- E. Use AWS Key Management Service (AWS KMS) for key managemen
- F. Create an S3 bucket policy to deny any PutObject command with a condition for x-amz-meta-side- encryption.
- G. Use AWS Key Management Service (AWS KMS) for key managemen
- H. Create an S3 bucket policy to deny any PutObject command with a condition for x-amz-server-side- encryption.

Answer: BDF

NEW QUESTION 49

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 50

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 Config
- 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 pattern
- 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 data
- F. Create an Amazon EventBridge rule to send notifications to the SNS topic.
- G. Enable Amazon GuardDuty
- 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 53

A company runs ECS services behind an internet-facing ALB that is the origin for CloudFront. An AWS WAF web ACL is associated with CloudFront, but clients can bypass it by accessing the ALB directly.

Which solution will prevent direct access to the ALB?

- A. Use AWS PrivateLink with the ALB.
- B. Replace the ALB with an internal ALB.
- C. Restrict ALB listener rules to CloudFront IP ranges.
- D. Require a custom header from CloudFront and validate it at the ALB.

Answer: D

NEW QUESTION 57

A company must inventory sensitive data across all Amazon S3 buckets in all accounts from a single security account.

- A. Delegate Amazon Macie and Security Hub administration.
- B. Use Amazon Inspector with Security Hub.
- C. Use Inspector with Trusted Advisor.
- D. Use Macie with Trusted Advisor.

Answer: A

NEW QUESTION 58

A security engineer is designing a solution that will provide end-to-end encryption between clients and Docker containers running in Amazon Elastic Container Service (Amazon ECS). This solution must also handle volatile traffic patterns.

Which solution would have the MOST scalability and LOWEST latency?

- A. Configure a Network Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers.
- B. Configure an Application Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers.
- C. Configure a Network Load Balancer with a TCP listener to pass through TLS traffic to the containers.
- D. Configure Amazon Route 53 to use multivalued answer routing to send traffic to the containers.

Answer: C

NEW QUESTION 59

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SCS-C03 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SCS-C03 Product From:

<https://www.2passeasy.com/dumps/SCS-C03/>

Money Back Guarantee

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