

# Amazon-Web-Services

## Exam Questions SCS-C03

AWS Certified Security - Specialty



#### NEW QUESTION 1

A company has a large fleet of Amazon Linux 2 Amazon EC2 instances that run an application processing sensitive data. Compliance requirements include no exposed management ports, full session logging, and authentication through AWS IAM Identity Center. DevOps engineers occasionally need access for troubleshooting.

Which solution will provide remote access while meeting these requirements?

- A. Grant access to the EC2 serial console and allow IAM role access.
- B. Enable EC2 Instance Connect and configure security groups accordingly.
- C. Assign an EC2 instance role that allows access to AWS Systems Manager
- D. Create an IAM policy that grants access to Systems Manager Session Manager and assign it to an IAM Identity Center role.
- E. Use Systems Manager Automation to temporarily open remote access ports.

**Answer: C**

#### 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's developers are using AWS Lambda function URLs to invoke functions directly. The company must ensure that developers cannot configure or deploy unauthenticated functions in production accounts. The company wants to meet this requirement by using AWS Organizations. The solution must not require additional work for the developers.

Which solution will meet these requirements?

- A. Require the developers to configure all function URLs to support cross-origin resource sharing (CORS) when the functions are called from a different domain.
- B. Use an AWS WAF delegated administrator account to view and block unauthenticated access to function URLs in production accounts, based on the OU of accounts that are using the functions.
- C. Use SCPs to allow all `lambda:CreateFunctionUrlConfig` and `lambda:UpdateFunctionUrlConfig` actions that have a `lambda:FunctionUrlAuthType` condition key value of `AWS_IAM`.
- D. Use SCPs to deny all `lambda:CreateFunctionUrlConfig` and `lambda:UpdateFunctionUrlConfig` actions that have a `lambda:FunctionUrlAuthType` condition key value of `NONE`.

**Answer: D**

#### NEW QUESTION 4

A company's application team needs a new AWS Key Management Service (AWS KMS) customer managed key to use with Amazon S3. The company's security policy requires separate keys for different AWS services to limit security exposure.

How can a security engineer limit the KMS customer managed key to work with only Amazon S3?

- A. Configure the key policy to allow only Amazon S3 to perform the `kms:Encrypt` action.
- B. Configure the key policy to allow KMS actions only when the value for the `kms:ViaService` condition key matches the Amazon S3 service name.
- C. Configure the application's IAM role policy to allow Amazon S3 to perform the `iam:PassRole` action.
- D. Configure the application's IAM role policy to allow only S3 operations when the operations are combined with the KMS customer managed key.

**Answer: B**

#### NEW QUESTION 5

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 6

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 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

An application is running on an Amazon EC2 instance that has an IAM role attached. The IAM role provides access to an AWS Key Management Service (AWS KMS) customer managed key and an Amazon S3 bucket. The key is used to access 2 TB of sensitive data that is stored in the S3 bucket. A security engineer discovers a potential vulnerability on the EC2 instance that could result in the compromise of the sensitive data. Due to other critical operations, the security engineer cannot immediately shut down the EC2 instance for vulnerability patching.

What is the FASTEST way to prevent the sensitive data from being exposed?

- A. Download the data from the existing S3 bucket to a new EC2 instance
- B. Then delete the data from the S3 bucket
- C. Re-encrypt the data with a client-based key
- D. Upload the data to a new S3 bucket.
- E. Block access to the public range of S3 endpoint IP addresses by using a host-based firewall
- F. Ensure that internet-bound traffic from the affected EC2 instance is routed through the host-based firewall.
- G. Revoke the IAM role's active session permission
- H. Update the S3 bucket policy to deny access to the IAM role
- I. Remove the IAM role from the EC2 instance profile.
- J. Disable the current key
- K. Create a new KMS key that the IAM role does not have access to, and re-encrypt all the data with the new key
- L. Schedule the compromised key for deletion.

**Answer:** C

#### NEW QUESTION 9

A company experienced a security incident caused by a vulnerable container image that was pushed from an external CI/CD pipeline into Amazon ECR. Which solution will prevent vulnerable images from being pushed?

- A. Enable ECR enhanced scanning with Lambda blocking.
- B. Use Amazon Inspector with EventBridge and Lambda.
- C. Integrate Amazon Inspector into the CI/CD pipeline using SBOM generation and fail the pipeline on critical findings.
- D. Enable basic continuous ECR scanning.

**Answer:** C

#### NEW QUESTION 10

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 10

An AWS Lambda function was misused to alter data, and a security engineer must identify who invoked the function and what output was produced. The engineer cannot find any logs created by the Lambda function in Amazon CloudWatch Logs. Which of the following explains why the logs are not available?

- A. The execution role for the Lambda function did not grant permissions to write log data to CloudWatch Logs.
- B. The Lambda function was invoked by using Amazon API Gateway, so the logs are not stored in CloudWatch Logs.
- C. The execution role for the Lambda function did not grant permissions to write to the Amazon S3 bucket where CloudWatch Logs stores the logs.
- D. The version of the Lambda function that was invoked was not current.

**Answer: A**

#### NEW QUESTION 15

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 19

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 20

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 23

A security engineer configured VPC Flow Logs to publish to Amazon CloudWatch Logs. After 10 minutes, no logs appear. The issue is isolated to the IAM role associated with VPC Flow Logs. What could be the reason?

- A. logs:GetLogEvents is missing.
- B. The engineer cannot assume the role.
- C. The vpc-flow-logs.amazonaws.com principal cannot assume the role.
- D. The role cannot tag the log stream.

**Answer: C**

#### NEW QUESTION 26

A company creates AWS Lambda functions from container images that are stored in Amazon Elastic Container Registry (Amazon ECR). The company needs to identify any software vulnerabilities in the container images and any code vulnerabilities in the Lambda functions. Which solution will meet these requirements?

- A. Enable Amazon GuardDuty
- B. Configure Amazon ECR scanning and Lambda code scanning in GuardDuty.
- C. Enable Amazon GuardDuty
- D. Configure Runtime Monitoring and Lambda Protection in GuardDuty.
- E. Enable Amazon Inspector
- F. Configure Amazon ECR enhanced scanning and Lambda code scanning in Amazon Inspector.
- G. Enable AWS Security Hub

H. Configure Runtime Monitoring and Lambda Protection in Security Hub.

**Answer: C**

#### NEW QUESTION 31

A company has a single AWS account and uses an Amazon EC2 instance to test application code. The company recently discovered that the instance was compromised and was serving malware. Analysis showed that the instance was compromised 35 days ago. A security engineer must implement a continuous monitoring solution that automatically notifies the security team by email for high severity findings as soon as possible. Which combination of steps should the security engineer take to meet these requirements? (Select THREE.)

- A. Enable AWS Security Hub in the AWS account.
- B. Enable Amazon GuardDuty in the AWS account.
- C. Create an Amazon Simple Notification Service (Amazon SNS) topic.
- D. Subscribe the security team's email distribution list to the topic.
- E. Create an Amazon Simple Queue Service (Amazon SQS) queue.
- F. Subscribe the security team's email distribution list to the queue.
- G. Create an Amazon EventBridge rule for GuardDuty findings of high severity.
- H. Configure the rule to publish a message to the topic.
- I. Create an Amazon EventBridge rule for Security Hub findings of high severity.
- J. Configure the rule to publish a message to the queue.

**Answer: BCE**

#### NEW QUESTION 32

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 33

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 36

A consultant agency needs to perform a security audit for a company's production AWS account. Several consultants need access to the account. The consultant agency already has its own AWS account. The company requires multi-factor authentication (MFA) for all access to its production account. The company also forbids the use of long-term credentials.

Which solution will provide the consultant agency with access that meets these requirements?

- A. Create an IAM group.
- B. Create an IAM user for each consultant.
- C. Add each user to the group.
- D. Turn on MFA for each consultant.
- E. Configure Amazon Cognito on the company's production account to authenticate against the consultant agency's identity provider (IdP). Add MFA to a Cognito user pool.
- F. Create an IAM role in the consultant agency's AWS account.
- G. Define a trust policy that requires MFA.
- H. In the trust policy, specify the company's production account as the principal.
- I. Attach the trust policy to the role.
- J. Create an IAM role in the company's production account.
- K. Define a trust policy that requires MFA.
- L. In the trust policy, specify the consultant agency's AWS account as the principal.
- M. Attach the trust policy to the role.

**Answer: D**

#### NEW QUESTION 41

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 Advisor
- B. Configure all the Trusted Advisor checks
- C. Manually map the checks against the PCI DSS v4.0 standard to generate the report.
- D. Enable and configure AWS Config
- E. Deploy the Operational Best Practices for PCI DSS conformance pack in AWS Config
- F. Use AWS Config to generate the report.
- G. Enable AWS Security Hub
- H. Enable the Security Hub PCI DSS security standard
- 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 framework
- K. Add all evidence to the assessment
- L. Generate the report in Audit Manager for download.

**Answer:** D

#### NEW QUESTION 44

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 47

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 keys.
- 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-north-1. Change the application code to point to the alias for eu-north-1.

**Answer:** C

#### NEW QUESTION 52

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 53

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 54

A company runs a global e-commerce 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 58**

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 59**

A company runs a public web application on Amazon EKS behind Amazon CloudFront and an Application Load Balancer (ALB). A security engineer must send a notification to an existing Amazon SNS topic when the application receives 10,000 requests from the same end-user IP address within any 5-minute period. Which solution will meet these requirements?

- A. Configure CloudFront standard logging and CloudWatch Logs metric filters.
- B. Configure VPC Flow Logs and CloudWatch Logs metric filters.
- C. Configure an AWS WAF web ACL with an ASN match rule and CloudWatch alarms.
- D. Configure an AWS WAF web ACL with a rate-based rule.
- E. Associate it with CloudFront.
- F. Create a CloudWatch alarm to notify SNS.

**Answer: D**

**NEW QUESTION 64**

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 67**

A company needs to detect unauthenticated access to its Amazon Elastic Kubernetes Service (Amazon EKS) clusters. The solution must require no additional configuration of the existing EKS deployment. Which solution will meet these requirements with the LEAST operational effort?

- A. Install a third-party security add-on.
- B. Enable AWS Security Hub and monitor Kubernetes findings.
- C. Monitor CloudWatch Container Insights metrics for EKS.
- D. Enable Amazon GuardDuty and use EKS Audit Log Monitoring.

**Answer: D**

**NEW QUESTION 71**

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 76**

.....

## **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](#)**