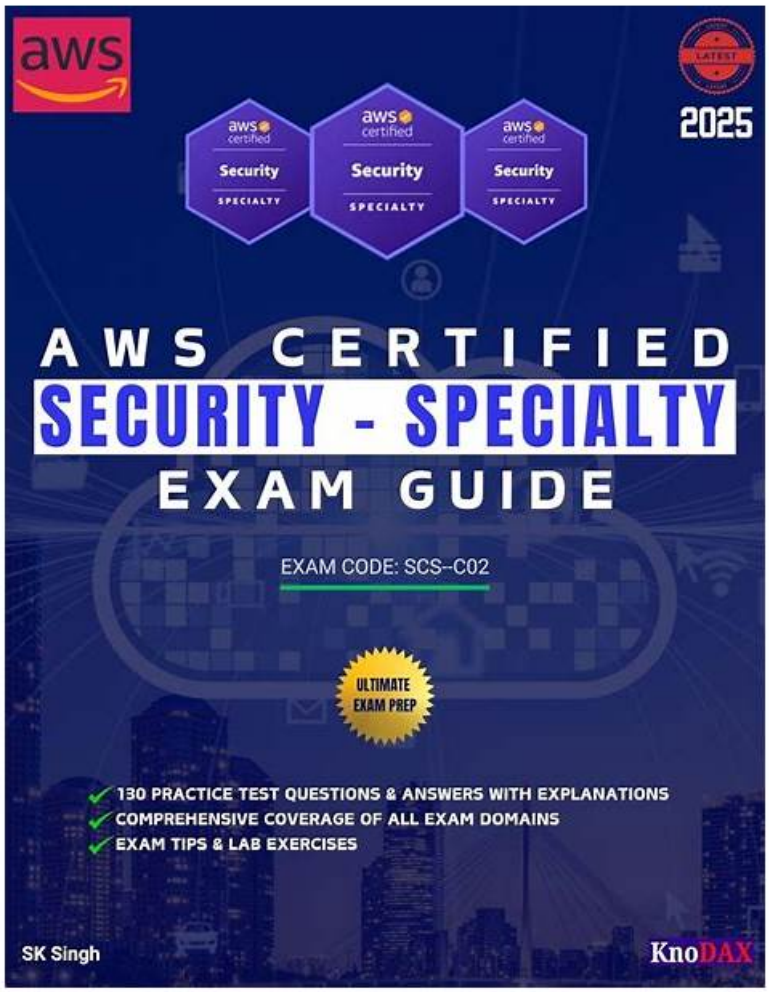
SCS-C02 Test Online & SCS-C02 Reliable Exam Pass4sure



2025 Latest ExamsLabs SCS-C02 PDF Dumps and SCS-C02 Exam Engine Free Share: https://drive.google.com/open?id=1ctFA7MWnhNQ8eSRZLm1MYfLLyDlu4Zci

Our SCS-C02 training guide always promise the best to service the clients. We are committing in this field for many years and have a good command of the requirements of various candidates. Carefully testing and producing to match the certified quality standards of SCS-C02 Exam Materials, we have made specific statistic researches on the SCS-C02 practice materials. And our pass rate of the SCS-C02 study engine is high as 98% to 100%.

Amazon SCS-C02 Exam Syllabus Topics:

Topic	Details
Topic 1	• Threat Detection and Incident Response: In this topic, AWS Security specialists gain expertise in crafting incident response plans and detecting security threats and anomalies using AWS services. It delves into effective strategies for responding to compromised resources and workloads, ensuring readiness to manage security incidents. Mastering these concepts is critical for handling scenarios assessed in the SCS-C02 exam.
Topic 2	• Infrastructure Security: Aspiring AWS Security specialists are trained to implement and troubleshoot security controls for edge services, networks, and compute workloads under this topic. Emphasis is placed on ensuring resilience and mitigating risks across AWS infrastructure. This section aligns closely with the exam's focus on safeguarding critical AWS services and environments.

Topic 3	• Identity and Access Management: The topic equips AWS Security specialists with skills to design, implement, and troubleshoot authentication and authorization mechanisms for AWS resources. By emphasizing secure identity management practices, this area addresses foundational competencies required for effective access control, a vital aspect of the certification exam.
Topic 4	• Security Logging and Monitoring: This topic prepares AWS Security specialists to design and implement robust monitoring and alerting systems for addressing security events. It emphasizes troubleshooting logging solutions and analyzing logs to enhance threat visibility.

SCS-C02 Reliable Exam Pass4sure & Latest SCS-C02 Mock Exam

Our company abides by the industry norm all the time. By virtue of the help from professional experts, who are conversant with the regular exam questions of our latest real dumps. The AWS Certified Security - Specialty exam dumps have summarized some types of questions in the qualification examination, so that users will not be confused when they take part in the exam, to have no emphatic answers. It can be said that the template of these questions can be completely applied. The user only needs to write out the routine and step points of the SCS-C02 test material, so that we can get good results in the exams.

Amazon AWS Certified Security - Specialty Sample Questions (Q111-Q116):

NEW QUESTION # 111
A security team is working on a solution that will use Amazon EventBridge (Amazon CloudWatch Events) to monitor new Amazon S3 objects. The solution will monitor for public access and for changes to any S3 bucket policy or setting that result in public access. The security team configures EventBridge to watch for specific API calls that are logged from AWS CloudTrail. EventBridge has an action to send an email notification through Amazon Simple Notification Service (Amazon SNS) to the security team immediately with details of the API call.
Specifically, the security team wants EventBridge to watch for the s3:PutObjectAcl, s3:DeleteBucketPolicy, and s3:PutBucketPolicy API invocation logs from CloudTrail. While developing the solution in a single account, the security team discovers that the s3:PutObjectAcl API call does not invoke an EventBridge event.
However, the s3:DeleteBucketPolicy API call and the s3:PutBucketPolicy API call do invoke an event.
The security team has enabled CloudTrail for AWS management events with a basic configuration in the AWS Region in which EventBridge is being tested. Verification of the EventBridge event pattern indicates that the pattern is set up correctly. The security team must implement a solution so that the s3:PutObjectAcl API call will invoke an EventBridge event. The solution must not generate false notifications.
Which solution will meet these requirements?

- A. Enable CloudTrail Insights to identify unusual API activity.
- B. Enable CloudTrail to monitor data events for read and write operations to S3 buckets.
- C. Modify the EventBridge event pattern by selecting Amazon S3. Select All Events as the event type.
- D. Modify the EventBridge event pattern by selecting Amazon S3. Select Bucket Level Operations as the event type.

Answer: B

Explanation:
The correct answer is D. Enable CloudTrail to monitor data events for read and write operations to S3 buckets.
According to the AWS documentation1, CloudTrail data events are the resource operations performed on or within a resource. These are also known as data plane operations. Data events are often high-volume activities. For example, Amazon S3 object-level API activity (such as GetObject, DeleteObject, and PutObject) is a data event.
By default, trails do not log data events. To record CloudTrail data events, you must explicitly add the supported resources or resource types for which you want to collect activity. For more information, see Logging data events in the Amazon S3 User Guide2.
In this case, the security team wants EventBridge to watch for the s3:PutObjectAcl API invocation logs from CloudTrail. This API uses the acl subresource to set the access control list (ACL) permissions for a new or existing object in an S3 bucket3. This is a data event that affects the S3 object resource type. Therefore, the security team must enable CloudTrail to monitor data events for read and write operations to S3 buckets in order to invoke an EventBridge event for this API call.
The other options are incorrect because:

* A. Modifying the EventBridge event pattern by selecting Amazon S3 and All Events as the event type will not capture the s3:PutObjectAcl API call, because this is a data event and not a management event.
Management events provide information about management operations that are performed on resources in your AWS account. These are also known as control plane operations4.
* B. Modifying the EventBridge event pattern by selecting Amazon S3 and Bucket Level Operations as the event type will not capture the s3:PutObjectAcl API call, because this is a data event that affects the S3 object resource type and not the S3 bucket resource type. Bucket level operations are management events that affect the configuration or metadata of an S3 bucket5.
* C. Enabling CloudTrail Insights to identify unusual API activity will not help the security team monitor new S3 objects or changes to any S3 bucket policy or setting that result in public access. CloudTrail Insights helps AWS users identify and respond to unusual activity associated with API calls and API error rates by continuously analyzing CloudTrail management events6. It does not analyze data events or generate EventBridge events.
References:
1: CloudTrail log event reference - AWS CloudTrail 2: Logging data events - AWS CloudTrail 3: PutObjectAcl - Amazon Simple Storage Service 4: [Logging management events - AWS CloudTrail] 5: [Amazon S3 Event Types - Amazon Simple Storage Service] 6: Logging Insights events for trails - AWS CloudTrail

NEW QUESTION # 112
A security engineer needs to configure an Amazon S3 bucket policy to restrict access to an S3 bucket that is named DOC-EXAMPLE-BUCKET. The policy must allow access to only DOC-EXAMPLE-BUCKET from only the following endpoint: vpce-1a2b3c4d. The policy must deny all access to DOC-EXAMPLE-BUCKET if the specified endpoint is not used.
Which bucket policy statement meets these requirements?

- A. A computer code with black text Description automatically generated

```
"Statement": [
    {
        "Sid": "Access-to-specific-VPCE-only",
        "Principal": "*",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": ["arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                     "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"],
        "Condition": {
            "StringEquals": {
                "aws:sourceVpce": "vpce-1a2b3c4d"
            }
        }
    }
]
```

- B. A computer code with black text Description automatically generated

```
"Statement": [
    {
        "Sid": "Access-to-specific-VPCE-only",
        "Principal": "*",
        "Action": "s3:*",
        "Effect": "Allow",
        "Resource": ["arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                     "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"],
        "Condition": {
            "StringNotEquals": {
                "aws:sourceVpce": "vpce-1a2b3c4d"
            }
        }
    }
]
```

- C. A computer code with black text Description automatically generated

- D. A computer code with black text Description automatically generated

Answer: C

Explanation:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies-vpc-endpoint.html

NEW QUESTION # 113
A security team is developing an application on an Amazon EC2 instance to get objects from an Amazon S3 bucket. All objects in the S3 bucket are encrypted with an AWS Key Management Service (AWS KMS) customer managed key. All network traffic for requests that are made within the VPC is restricted to the AWS infrastructure. This traffic does not traverse the public internet.
The security team is unable to get objects from the S3 bucket
Which factors could cause this issue? (Select THREE.)

- A. The IAM instance profile that is attached to the EC2 instance does not allow the s3 ListBucket action to the S3: bucket in the AWS accounts.
- B. The KMS key policy that encrypts the object in the S3 bucket does not allow the kms; ListKeys action to the EC2 instance profile ARN.
- C. The I AM instance profile that is attached to the EC2 instance does not allow the s3 ListParts action to the S3; bucket in the AWS accounts.
- D. The security group that is attached to the EC2 instance is missing an outbound rule to the S3 managed prefix list over port 443.
- E. The KMS key policy that encrypts the object in the S3 bucket does not allow the kms Decrypt action to the EC2 instance profile ARN.
- F. The security group that is attached to the EC2 instance is missing an inbound rule from the S3 managed prefix list over port

443.

Answer: A,D,E

Explanation:
https://docs.aws.amazon.com/vpc/latest/userguide/security-group-rules.html To get objects from an S3 bucket that are encrypted with a KMS customer managed key, the security team needs to have the following factors in place:
The IAM instance profile that is attached to the EC2 instance must allow the s3:GetObject action to the S3 bucket or object in the AWS account. This permission is required to read the object from S3. Option A is incorrect because it specifies the s3:ListBucket action, which is only required to list the objects in the bucket, not to get them.
The KMS key policy that encrypts the object in the S3 bucket must allow the kms:Decrypt action to the EC2 instance profile ARN. This permission is required to decrypt the object using the KMS key.Option D is correct.
The security group that is attached to the EC2 instance must have an outbound rule to the S3 managed prefix list over port 443. This rule is required to allow HTTPS traffic from the EC2 instance to S3 within the AWS infrastructure. Option E is correct. Option B is incorrect because it specifies the s3:ListParts action, which is only required for multipart uploads, not for getting objects. Option C is incorrect because it specifies the kms:
ListKeys action, which is not required for getting objects. Option F is incorrect because it specifies an inbound rule from the S3 managed prefix list, which is not required for getting objects.Verified References:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingKMSEncryption.html
https://docs.aws.amazon.com/kms/latest/developerguide/control-access.html
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html

NEW QUESTION # 114
A company's Chief Security Officer has requested that a Security Analyst review and improve the security posture of each company IAM account The Security Analyst decides to do this by Improving IAM account root user security.
Which actions should the Security Analyst take to meet these requirements? (Select THREE.)

- A. Create an admin IAM user with administrative privileges and delete the account root user in every account.
- B. Create a custom IAM policy to limit permissions to required actions for the account root user and attach the policy to the account root user.
- C. Attach an IAM role to the account root user to make use of the automated credential rotation in IAM STS.
- D. Delete the access keys for the account root user in every account.
- E. Enable multi-factor authentication (MFA) on every account root user in all accounts.
- F. Implement a strong password to help protect account-level access to the IAM Management Console by the account root user.

Answer: B,D,E

Explanation:
because these are the actions that can improve IAM account root user security. IAM account root user is a user that has complete access to all AWS resources and services in an account. IAM account root user security is a set of best practices that help protect the account root user from unauthorized or accidental use. Deleting the access keys for the account root user in every account can help prevent programmatic access by the account root user, which reduces the risk of compromise or misuse. Enabling MFA on every account root user in all accounts can help add an extra layer of security for console access by requiring a verification code in addition to a password. Creating a custom IAM policy to limit permissions to required actions for the account root user and attaching the policy to the account root user can help enforce the principle of least privilege and restrict the account root user from performing unnecessary or dangerous actions. The other options are either invalid or ineffective for improving IAM account root user security.

NEW QUESTION # 115
A company receives a notification from the AWS Abuse team about an AWS account The notification indicates that a resource in the account is compromised The company determines that the compromised resource is an Amazon EC2 instance that hosts a web application The compromised EC2 instance is part of an EC2 Auto Scaling group The EC2 instance accesses Amazon S3 and Amazon DynamoDB resources by using an 1AM access key and secret key The 1AM access key and secret key are stored inside the AMI that is specified in the Auto Scaling group's launch configuration The company is concerned that the credentials that are stored in the AMI might also have been exposed The company must implement a solution that remediates the security concerns without causing downtime for the application The solution must comply with security best practices Which solution will meet these requirements'?

- A. Rotate the potentially compromised access key Create a new AMI without the potentially compromised access key Use a user data script to supply the new access key as environmental variables in the Auto Scaling group's launch configuration Perform an EC2 Auto Scaling instance refresh
- B. Delete or deactivate the potentially compromised access key Create a new AMI without the potentially compromised credentials Create an 1AM role that includes the correct permissions Create a launch template for the Auto Scaling group to reference the new AMI and 1AM role Perform an EC2 Auto Scaling instance refresh
- C. Rotate the potentially compromised access key that the EC2 instance uses Create a new AM I without the potentially compromised credentials Perform an EC2 Auto Scaling instance refresh
- D. Delete or deactivate the potentially compromised access key Create an EC2 Auto Scaling linked 1AM role that includes a custom policy that matches the potentially compromised access key permission Associate the new 1AM role with the Auto Scaling group Perform an EC2 Auto Scaling instance refresh.

Answer: B

Explanation:
The AWS documentation states that you can create a new AMI without the potentially compromised credentials and create an 1AM role that includes the correct permissions. You can then create a launch template for the Auto Scaling group to reference the new AMI and 1AM role. This method is the most secure way to remediate the security concerns without causing downtime for the application.
References: : AWS Security Best Practices

NEW QUESTION # 116
......

The SCS-C02 examination certification, as other world-renowned certification, will get international recognition and acceptance. People around the world prefer SCS-C02 exam certification to make their careers more strengthened and successful. In ExamsLabs, you can choose the products which are suitable for your learning ability to learn.

harunfloor.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

What's more, part of that ExamsLabs SCS-C02 dumps now are free: https://drive.google.com/open?id=1ctFA7MWnhNQ8eSRZLm1MYfLLyDlu4Zci