Reliable SCS-C03 Exam Cram & Exam Questions SCS-C03 Vce

Pass4Leader Amazon exam study material can simulate the actual test and give you an interactive experience during the practice. When you choose our SCS-C03 valid training dumps, you will enjoy one year free update for SCS-C03 Pdf Torrent without any additional cost. These updates are meant to reflect any changes related to the SCS-C03 actual test. 100% pass is an easy thing for you.

Amazon SCS-C03 Exam Syllabus Topics:

Topic	Details
Topic 1	• Identity and Access Management: This domain deals with controlling authentication and authorization through user identity management, role-based access, federation, and implementing least privilege principles.
Topic 2	• Infrastructure Security: This domain focuses on securing AWS infrastructure including networks, compute resources, and edge services through secure architectures, protection mechanisms, and hardened configurations.
Topic 3	• Data Protection: This domain centers on protecting data at rest and in transit through encryption, key management, data classification, secure storage, and backup mechanisms.
Topic 4	• Incident Response: This domain addresses responding to security incidents through automated and manual strategies, containment, forensic analysis, and recovery procedures to minimize impact and restore operations.
Topic 5	• Security Foundations and Governance: This domain addresses foundational security practices including policies, compliance frameworks, risk management, security automation, and audit procedures for AWS environments.

>> Reliable SCS-C03 Exam Cram <<

Quiz SCS-C03 - AWS Certified Security - Specialty –The Best Reliable Exam Cram

Our product provides the demo thus you can have a full understanding of our SCS-C03 prep torrent. You can visit the pages of the product and then know the version of the product, the characteristics and merits of the SCS-C03 test braindumps, the price of the product and the discount. There are also the introduction of the details and the guarantee of our SCS-C03 prep torrent for you to read. You can also know how to contact us and what other client's evaluations about our SCS-C03 test braindumps. You will pass the SCS-C03 exam as our SCS-C03 study gude has a pass rate of 99% to 100%.

Amazon AWS Certified Security - Specialty Sample Questions (Q209-Q214):

NEW QUESTION # 209
A company has enabled AWS Config for its organization in AWS Organizations. The company has deployed hundreds of Amazon S3 buckets across the organization. A security engineer needs to identify any S3 buckets that are not encrypted with AWS Key Management Service (AWS KMS). The security engineer also must prevent objects that are not encrypted with AWS KMS from being uploaded to the S3 buckets.
Which solution will meet these requirements?

- A. Use thes3-bucket-ssl-requests-onlyAWS Config managed rule to identify unencrypted S3 buckets.Create bucket policies for each S3 bucket to allow thes3:PutObjectaction only when the object is encrypted with AWS KMS.
- B. Use thes3-bucket-ssl-requests-onlyAWS Config managed rule to identify unencrypted S3 buckets.
  Create an SCP to allow thes3:PutObjectaction only when the object is encrypted with AWS KMS.
- C. Use thes3-default-encryption-kmsAWS Config managed rule to identify unencrypted S3 buckets.
  Create bucket policies for each S3 bucket to deny thes3:PutObjectaction only when the object has server-side encryption with S3 managed keys (SSE-S3).
- D. Use thes3-default-encryption-kmsAWS Config managed rule to identify unencrypted S3 buckets.
  Create an SCP to allow thes3:PutObjectaction only when the object is encrypted with AWS KMS.

Answer: D

Explanation:
The correct Config rule for finding buckets that are not usingSSE-KMS by defaultiss3-default-encryption- kms. It evaluates the bucket's default encryption settings and flags buckets that do not have KMS default encryption enabled. The s3-bucket-ssl-requests-only rule focuses on enforcing HTTPS-only requests and does not validate encryption-at-rest settings, so it cannot satisfy the "identify not encrypted with KMS" requirement.
For preventing uploads of objects that are not encrypted with KMS, an organization-wide control is needed.
AnSCPcan restrict s3:PutObject so that uploads succeed only when the request specifiesSSE-KMS(and optionally a specific KMS key). This provides broad, low-touch enforcement across many accounts and buckets. While bucket policies can also enforce SSE-KMS, managing and verifying hundreds of bucket policies is more operationally heavy than a centrally managed SCP guardrail.
Option B enforcesSSE-S3, which does not meet the requirement forKMSencryption. Option D uses the wrong Config rule and relies on an "allow-only" pattern rather than explicit deny logic, making it an unreliable fit for the stated goal. Therefore, A is the best answer.

NEW QUESTION # 210
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. Enable PublicAccessBlock and deny s3:PutPublicAccessBlock by SCP.
- B. Enable PublicAccessBlock and deny s3:GetObject by SCP.
- C. Enable Object Lock governance and deny s3:PutPublicAccessBlock by SCP.
- D. Enforce KMS encryption and deny s3:GetObject by SCP.

Answer: A

Explanation:
Amazon S3 Block Public Access provides centralized controls to prevent public access through bucket policies and ACLs. AWS Certified Security - Specialty guidance recommends enabling Block Public Access to reduce accidental exposure and to enforce guardrails that override public grants. Enabling Block Public Access on the bucket removes current public exposure when combined with correcting policies/ACLs and prevents future misconfiguration. To ensure the bucket cannot be made public again, the security engineer must prevent principals from disabling Block Public Access. An SCP that denies s3:PutPublicAccessBlock prevents changes that would remove or weaken the PublicAccessBlock configuration, enforcing the guardrail across the OU or account.
Options A and D do not directly address public exposure control. Option B denies object reads but does not ensure public access cannot be re-enabled; it also does not address the root misconfiguration pathways and could disrupt legitimate access patterns.
Option C specifically combines the correct preventive control (PublicAccessBlock) with organizational enforcement to stop future reversal.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
Amazon S3 Block Public Access

AWS Organizations SCP Guardrails for S3 Controls

NEW QUESTION # 211
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 CloudWatch Logs. Use a subscription filter to match logs with detection rules and to send alerts to the SNS topic. Search the logs manually by using CloudWatch Logs Insights.
- B. Analyze the logs by using Amazon OpenSearch Service. Search the logs from the OpenSearch API.
  Use OpenSearch Service Security Analytics to match logs with detection rules and to send alerts to the SNS topic.
- C. Analyze the logs by using AWS Security Hub. Search the logs from the Findings page in Security Hub.
  Create custom actions to match logs with detection rules and to send alerts to the SNS topic.
- D. Analyze the logs by using Amazon QuickSight. Search the logs by listing the query results in a dashboard. Run queries to match logs with detection rules and to send alerts to the SNS topic.

Answer: B

Explanation:
Amazon OpenSearch Service is designed for near real-time log ingestion, indexing, and search across large volumes of data.
According to the AWS Certified Security - Specialty Study Guide, OpenSearch supports advanced log analytics use cases and integrates with OpenSearch Security Analytics, which provides prebuilt and custom detection rules.
Security Analytics can continuously evaluate incoming logs from multiple AWS services and generate alerts when detection rules are matched. These alerts can be forwarded to Amazon SNS with minimal configuration.
OpenSearch also provides powerful search and query capabilities through APIs and dashboards.
Option C supports detection but lacks advanced correlation and scalable search capabilities. Option B is not a log analytics service.
Option D is a visualization service and does not support real-time detection.
AWS guidance recommends OpenSearch Service for centralized, near real-time log analysis and alerting.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
Amazon OpenSearch Service Security Analytics
AWS Logging and Monitoring Architecture

NEW QUESTION # 212
A company uploads data files as objects into an Amazon S3 bucket. A vendor downloads the objects to perform data processing.
A security engineer must implement a solution that prevents objects from residing in the S3 bucket for longer than 72 hours.

- A. Generate presigned URLs that expire after 72 hours.
- B. Configure S3 Versioning to expire object versions that have been in the bucket for 72 hours.
- C. Use the S3 Intelligent-Tiering storage class and configure expiration after 72 hours.
- D. Configure an S3 Lifecycle configuration rule on the bucket to expire objects after 72 hours.

Answer: D

Explanation:
Amazon S3 Lifecycle configuration rules are the native, automated mechanism for managing object retention and deletion. According to AWS Certified Security - Specialty documentation, lifecycle rules can be configured to expire objects based on the number of days since object creation. Once the expiration time is reached, Amazon S3 permanently deletes the objects without manual intervention.
This solution directly enforces a maximum retention period of 72 hours and ensures compliance regardless of whether the vendor downloads the data or not. Lifecycle rules are evaluated continuously by Amazon S3 and do not require scripts, cron jobs, or additional services, making them the most operationally efficient and cost- effective solution.
S3 Versioning controls versions but does not enforce object deletion timelines. S3 Intelligent-Tiering optimizes storage cost but does not delete objects. Presigned URLs only control access duration and do not remove objects from storage.
AWS explicitly recommends lifecycle policies for automated data retention enforcement.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
Amazon S3 Lifecycle Management

NEW QUESTION # 213
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 the following key policy to allow the infrastructure deployment team to create encrypted Amazon Elastic Block Store (Amazon EBS) volumes by assuming the InfrastructureDeployment IAM role:

```
{
"Version": "2012-10-17",
"Id": "key-policy-ebs",
"Statement": [
{
"Sid": "Enable IAM User Permissions",
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::123456789012:root"
},
"Action": "kms:*",
"Resource": "*"
},
{
"Sid": "Allow use of the key",
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::123456789012:role/aws-reserved/sso.amazonaws.com/InfrastructureDeployment"
},
"Action": [
"kms:Encrypt",
"kms:Decrypt",
"kms:ReEncrypt*",
"kms:GenerateDataKey*",
"kms:DescribeKey",
"kms:CreateGrant",
"kms:ListGrants",
"kms:RevokeGrant"
],
"Resource": "*",
"Condition": {
"StringEquals": {
"kms:ViaService": "ec2.us-west-2.amazonaws.com"
}
}
}
]
}
```

The security engineer recently discovered that IAM rolesother thanthe 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 policy document, add a new statement block that grants the kms:Disable* permission to the security engineer's IAM role.
- 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 theConditionblock, change the kms:ViaService value to ec2.us-east-1.amazonaws.com.
- D. In the statement block that contains the Sid"Allow use of the key", under theConditionblock, change StringEquals to StringLike.

Answer: D

Explanation:
AWS KMS key policies can restrict how and when a key is used by applyingconditions such as kms:
ViaService, which limits usage to requests that originate from a specific AWS service. According to the AWS Certified Security -

Specialty Official Study Guide and AWS KMS documentation, the kms:ViaService condition is evaluated against the service that calls KMS on behalf of the principal.
Using StringEquals with kms:ViaService restricts usage toexactly one service endpoint. However, AWS services can invoke KMS throughservice variants, internal endpoints, or additional service integrations.
When StringEquals is used, these variations can unintentionally bypass the condition, allowing the key to be used by other services through different internal service paths.
Changing the condition operator from StringEquals to StringLike ensures thatonly EC2-related service calls that match the intended service pattern are allowed, while still preventing use by unrelated AWS services.
This aligns with AWS guidance to use StringLike when service invocation patterns may vary.
Option B is incorrect because the root principal statement is required to retain administrative control over the key. Option C is invalid because changing Regions does not address unauthorized service usage. Option D does not restrict key usage and does not mitigate the issue.
AWS documentation explicitly recommendstightening condition operatorsin KMS key policies to prevent unintended service access while maintaining required functionality.
* AWS Certified Security - Specialty Official Study Guide
* AWS Key Management Service Developer Guide
* AWS KMS Key Policy Best Practices

NEW QUESTION # 214
.....

Attending training institution or having Amazon online training classes may be a good choice for candidates. But for people who have no time and energy to prepare for SCS-C03 practice exam, training calss will make them tired and exhausted. The most effective way for them to pass SCS-C03 Actual Test is choosing best study materials that you will find in Pass4Leader.