Quiz 2026 Amazon SCS-C02: AWS Certified Security - Specialty High Hit-Rate Visual Cert Exam

P.S. Free 2026 Amazon SCS-C02 dumps are available on Google Drive shared by Pass4SureQuiz: https://drive.google.com/open?id=1EOPylFkXSVeHRiY0zHldpzBGArZcqToz

You only need 20-30 hours to learn our SCS-C02 test braindumps and then you can attend the exam and you have a very high possibility to pass the exam. For many people whether they are the in-service staff or the students they are busy in their job, family lives and other things. But you buy our SCS-C02 prep torrent you can mainly spend your time energy and time on your job, the learning or family lives and spare little time every day to learn our AWS Certified Security - Specialty exam torrent. Our answers and questions are compiled elaborately and easy to be mastered. Because our SCS-C02 Test Braindumps are highly efficient and the passing rate is very high you can pass the exam fluently and easily with little time and energy needed.

If you want to pass the exam quickly, our SCS-C02 practice engine is your best choice. We know that many users do not have a large amount of time to learn. In response to this, we have scientifically set the content of the SCS-C02 exam questions. On one hand, we have collected the most important keypoints which will definitely show up in the real exam to the content of the SCS-C02 learning guide. On the other hand, we have simplified the content and make it better to be understood by all of the customers.

>> SCS-C02 Visual Cert Exam <<

Knowledge SCS-C02 Points & SCS-C02 Reliable Test Camp

Pass4SureQuiz have a professional IT team to do research for practice questions and answers of the Amazon SCS-C02 exam certification exam. They provide a very effective training tools and online services for your. If you want to buy Pass4SureQuiz products, Pass4SureQuiz will provide you with the latest, the best quality and very detailed training materials as well as a very accurate exam practice questions and answers to be fully prepared for you to participate in the Amazon Certification SCS-C02 Exam. Safely use the questions provided by Pass4SureQuiz's products. Selecting the Pass4SureQuiz is equal to be 100% passing the exam.

Amazon SCS-C02 Exam Syllabus Topics:

Topic	Details
Topic 1	• Data Protection: AWS Security specialists learn to ensure data confidentiality and integrity for data in transit and at rest. Topics include lifecycle management of data at rest, credential protection, and cryptographic key management. These capabilities are central to managing sensitive data securely, reflecting the exam's focus on advanced data protection strategies.
Topic 2	• 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 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.

Amazon AWS Certified Security - Specialty Sample Questions (Q242-Q247):

NEW QUESTION # 242
To meet regulatory requirements, a Security Engineer needs to implement an IAM policy that restricts the use of AWS services to the us-east-1 Region.
What policy should the Engineer implement?

- A.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
          "Effect": "Deny",
          "Action": "*",
          "Resource": "*",
          "Condition":  {
              "StringNotEquals":  {
                  "aws:RequestedRegion": "us-east-1"
              }
          }
        }
    ]
}
```
- B.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
          "Effect": "Deny",
          "NotAction": "*",
          "Resource": "*",
          "Condition":  {
              "StringEquals":  {
                  "aws:RequestedRegion": "us-east-1'
              }
          }
        }
    ]
}
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*",
            "Condition":  {
                "StringEquals":  {
                    "aws:RequestedRegion": "us-east-1'
                }
            }
        }
    ]
```


- C.
- D.

Answer: A

Explanation:
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_aws_deny-requested-region.html

NEW QUESTION # 243
A company created an IAM account for its developers to use for testing and learning purposes Because MM account will be shared among multiple teams of developers, the company wants to restrict the ability to stop and terminate Amazon EC2 instances so that a team can perform these actions only on the instances it owns.
Developers were Instructed to tag al their instances with a Team tag key and use the team name in the tag value One of the first teams to use this account is Business Intelligence A security engineer needs to develop a highly scalable solution for providing developers with access to the appropriate resources within the account The security engineer has already created individual IAM roles for each team.
Which additional configuration steps should the security engineer take to complete the task?

- A. For each team, create an AM policy similar to the one that fellows Populate the ec2: ResourceTag/Team condition key with a proper team name Attach resulting policies to the corresponding IAM roles.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ]
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Team": "BusinessIntelligence"
                }
            }
        }
    ]
}
```

- B. Tag each IAM role with a Team lag key. and use the team name in the tag value. Create an IAM policy similar to the one that follows, and attach 4 to all the IAM roles used by developers.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Team": "${aws:PrincipalTag/Team}"
                }
            }
        }
    ]
}
```

- C. For each team create an IAM policy similar to the one that follows Populate the IAM TagKeys/Team condition key with a proper team name. Attach the resuming policies to the corresponding IAM roles.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys/Team": "BusinessIntelligence"
                }
            }
        }
    ]
}
```

- D. Tag each IAM role with the Team key, and use the team name in the tag value. Create an IAM policy similar to the one that follows, and it to all the IAM roles used by developers.

Answer: A

NEW QUESTION # 244
A company's policy requires that all API keys be encrypted and stored separately from source code in a centralized security account. This security account is managed by the company's security team However, an audit revealed that an API key is steed with the source code of an IAM Lambda function m an IAM CodeCommit repository in the DevOps account How should the security learn securely store the API key?

- A. Store the API key in an Amazon S3 bucket in the security account using server-side encryption with Amazon S3 managed encryption keys (SSE-S3) to encrypt the key Create a resigned URL tor the S3 key. and specify the URL m a Lambda environmental variable in the IAM CloudFormation template Update the Lambda function code to retrieve the key using the URL and call the API
- B. Create a CodeCommit repository in the security account using IAM Key Management Service (IAM KMS) tor encryption Require the development team to migrate the Lambda source code to this repository
- C. Create a secret in IAM Secrets Manager in the security account to store the API key using IAM Key Management Service (IAM KMS) tor encryption Grant access to the IAM role used by the Lambda function so that the function can retrieve the key from Secrets Manager and call the API
- D. Create an encrypted environment variable for the Lambda function to store the API key using IAM Key Management Service (IAM KMS) tor encryption Grant access to the IAM role used by the Lambda function so that the function can decrypt the key at runtime

Answer: C

Explanation:
Explanation
To securely store the API key, the security team should do the following:
Create a secret in AWS Secrets Manager in the security account to store the API key using AWS Key Management Service (AWS KMS) for encryption. This allows the security team to encrypt and manage the API key centrally, and to configure automatic rotation schedules for it.
Grant access to the IAM role used by the Lambda function so that the function can retrieve the key from Secrets Manager and call the API. This allows the security team to avoid storing the API key with the source code, and to use IAM policies to control access to the secret.

NEW QUESTION # 245
A company suspects that an attacker has exploited an overly permissive role to export credentials from Amazon EC2 instance metadata. The company uses Amazon GuardDuty and AWS Audit Manager. The company has enabled AWS CloudTrail logging

and Amazon CloudWatch logging for all of its AWS accounts.
A security engineer must determine if the credentials were used to access the company's resources from an external account.
Which solution will provide this information?

- A. Review CloudTrail logs for GetSessionToken API calls to AWS Security Token Service (AWS STS) that come from an acount ID from outside the company.
- B. Review GuardDuty findings to find InstanceCredentialExfiltration events.
- C. Review CloudWatch logs for GetSessionToken API calls to AWS Security Token Service (AWS STS) that come from an account ID from outside the company.
- D. Review assessment reports in the Audit Manager console to find InstanceCredentialExfiltration events.

Answer: B

Explanation:
The correct answer is A because GuardDuty can detect and alert on EC2 instance credential exfiltration events. These events indicate that the credentials obtained from the EC2 instance metadata service are being used from an IP address that is owned by a differentAWS account than the one that owns the instance1. GuardDuty can also provide details such as the source and destination IP addresses, the AWS account ID of the attacker, and the API calls made using the exfiltrated credentials2.
The other options are incorrect because they do not provide the information needed to determine if the credentials were used to access the company's resources from an external account. Option B is incorrect because Audit Manager does not generate InstanceCredentialExfiltration events. Audit Manager is a service that helpsyou continuously audit your AWS usage to simplify how you assess risk and compliance with regulations and industry standards3. Option C is incorrect because CloudTrail logs do not show the account ID of the caller for GetSessionToken API calls to AWS STS. CloudTrail logs show the account ID of the identity whose credentials were used to call the API4. Option D is incorrect because CloudWatch logs do not show the GetSessionToken API calls to AWS STS by default. CloudWatch logs can show the API calls made by AWS Lambda functions, Amazon API Gateway, and other AWS services that integrate with CloudWatch5.
Reference: InstanceCredentialExfiltration, Amazon GuardDuty Enhances Detection of EC2 Instance Credential Exfiltration, What Is AWS Audit Manager?, Logging AWS STS API Calls with AWS CloudTrail, What IsAmazon CloudWatch Logs?

NEW QUESTION # 246
A company is implementing new compliance requirements to meet customer needs. According to the new requirements, the company must not use any Amazon RDS DB instances or DB clusters that lack encryption of the underlying storage. The company needs a solution that will generate an email alert when an unencrypted DB instance or DB cluster is created. The solution also must terminate the unencrypted DB instance or DB cluster.
Which solution will meet these requirements in the MOST operationally efficient manner?

- A. Create an Amazon EventBridge rule that evaluates RDS event patterns and is initiated by the creation of DB instances or DB clusters. Configure the rule to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic that includes an AWS Lambda function and an email delivery target as subscribers. Configure the Lambda function to delete the unencrypted resource.
- B. Create an AWS Config managed rule to detect unencrypted RDS storage. Configure an automatic remediation action to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic that includes an AWS Lambda function and an email delivery target as subscribers. Configure the Lambda function to delete the unencrypted resource.
- C. Create an AWS Config managed rule to detect unencrypted RDS storage. Configure a manual remediation action to invoke an AWS Lambda function. Configure the Lambda function to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic and to delete the unencrypted resource.
- D. Create an Amazon EventBridge rule that evaluates RDS event patterns and is initiated by the creation of DB instances or DB clusters. Configure the rule to invoke an AWS Lambda function.Configure the Lambda function to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic and to delete the unencrypted resource.

Answer: B

Explanation:
Automatic configuration changes -> AWS Config

NEW QUESTION # 247
.....

according to the latest development in the theory and the practice so they are of great value. Please firstly try out our SCS-C02 training braindump before you decide to buy our SCS-C02 Study Guide as we have free demo on the web. It is worthy for you to buy our SCS-C02 exam preparation not only because it can help you pass the SCS-C02 exam successfully but also because it saves your time and energy.

Knowledge SCS-C02 Points: https://www.pass4surequiz.com/SCS-C02-exam-quiz.html

P.S. Free 2026 Amazon SCS-C02 dumps are available on Google Drive shared by Pass4SureQuiz: https://drive.google.com/open?id=1EOPylFkXSVeHRiY0zHldpzBGArZcqToz