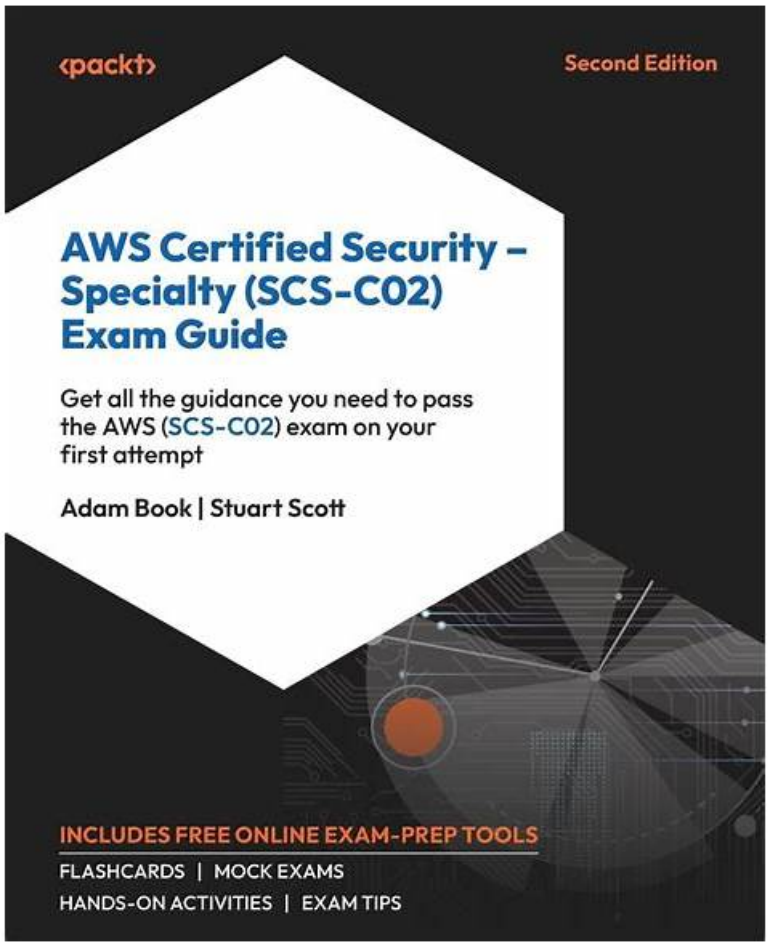
Amazon SCS-C02 Exams & Free SCS-C02 Learning Cram



2026 Latest Easy4Engine SCS-C02 PDF Dumps and SCS-C02 Exam Engine Free Share: https://drive.google.com/open?id=1KVyB6N_MVxKolc0srgd8pIqfCc5m8eP2

We aim to provide the best service on SCS-C02 exam questions for our customers, and we demand of ourselves and our after sale service staffs to the highest ethical standard, though our SCS-C02 study guide and compiling processes have been of the highest quality. We are deeply committed to meeting the needs of our customers, and we constantly focus on customer's satisfaction. We play an active role in making every customer in which we selling our SCS-C02 practice dumps a better place to live and work.

Amazon SCS-C02 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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 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.
Topic 5	• Management and Security Governance: This topic teaches AWS Security specialists to develop centralized strategies for AWS account management and secure resource deployment. It includes evaluating compliance and identifying security gaps through architectural reviews and cost analysis, essential for implementing governance aligned with certification standards.

Get the Latest SCS-C02 Exams for Immediate Study and Instant Success

With a high quality, we can guarantee that our SCS-C02 practice quiz will be your best choice. There are three different versions about our products, including the PDF version, the software version and the online version. The three versions are all good with same questions and answers; you can try to use the version of our SCS-C02 Guide materials that is suitable for you. Our SCS-C02 exam questions have many advantages, I am going to introduce you the main advantages of our SCS-C02 study materials, I believe it will be very beneficial for you and you will not regret to use our SCS-C02 learning guide.

Amazon AWS Certified Security - Specialty Sample Questions (Q57-Q62):

NEW QUESTION # 57
A company has a large fleet of Linux Amazon EC2 instances and Windows EC2 instances that run in private subnets. The company wants all remote administration to be performed as securely as possible in the AWS Cloud.
Which solution will meet these requirements?

- A. Do not use SSH-RSA private keys during the launch of new instances. Implement AWS Systems Manager Session Manager.
- B. Do not use SSH-RSA private keys during the launch of new instances. Configure EC2 Instance Connect.
- C. Generate new SSH-RSA private keys for existing instances. Configure EC2 Instance Connect.
- D. Generate new SSH-RSA private keys for existing instances. Implement AWS Systems Manager Session Manager.

Answer: A

Explanation:
AWS Systems Manager Session Manager is a fully managed service that allows you to securely and remotely administer your EC2 instances without the need to open inbound ports, maintain bastion hosts, or manage SSH keys. Session Manager provides an interactive browser-based shell or CLI access to your instances, as well as port forwarding and auditing capabilities. Session Manager works with both Linux and Windows instances, and supports hybrid environments and edge devices.
EC2 Instance Connect is a feature that allows you to use SSH to connect to your Linux instances using short-lived keys that are generated on demand and delivered securely through the AWS metadata service. EC2 Instance Connect does not require any additional software installation or configuration on the instance, but it does require you to use SSH-RSA keys during the launch of new instances.
The correct answer is to use Session Manager, as it provides more security and flexibility than EC2 Instance Connect, and does not require SSH-RSA keys or inbound ports. Session Manager also works with Windows instances, while EC2 Instance Connect does not.
Verified Reference:
https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Connect-using-EC2-Instance-Connect.html
https://repost.aws/questions/QUnV4R9EoeSdW0GT3cKBUR7w/what-is-the-difference-between-ec-2-instance-connect-and-session-manager-ssh-connections

NEW QUESTION # 58
A company has secured the AWS account root user for its AWS account by following AWS best practices. The company also has enabled AWS CloudTrail, which is sending its logs to Amazon S3. A security engineer wants to receive notification in near-real time if a user uses the AWS account root user credentials to sign in to the AWS Management Console.
Which solutions will provide this notification? (Select TWO.)

- A. Configure AWS CloudTrail to send its logs to Amazon CloudWatch Logs. Configure a metric filter on the CloudWatch Logs log group used by CloudTrail to evaluate log entries for successful root account logins. Create an Amazon CloudWatch alarm that monitors whether a root login has occurred Configure the CloudWatch alarm to notify an Amazon Simple Notification Service (Amazon SNS) topic when the alarm enters the ALARM state. Subscribe any required endpoints to this SNS topic so that these endpoints can receive notification.
- B. Configure AWS CloudTrail to send log notifications to an Amazon Simple Notification Service (Amazon SNS) topic. Create an AWS Lambda function that parses the CloudTrail notification for root login activity and notifies a separate SNS topic that contains the endpoints that should receive notification. Subscribe the Lambda function to the SNS topic that is receiving log notifications from CloudTrail.
- C. Configure an Amazon EventBridge event rule that runs when Amazon CloudWatch API calls are recorded for a successful root login. Configure the rule to target an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe any required endpoints to the SNS topic so that these endpoints can receive notification.
- D. Use AWS IAM Access Analyzer. Create an Amazon CloudWatch Logs metric filter to evaluate log entries from Access Analyzer that detect a successful root account login. Create an Amazon CloudWatch alarm that monitors whether a root login has occurred. Configure the CloudWatch alarm to notify an Amazon Simple Notification Service (Amazon SNS) topic when the alarm enters the ALARM state. Subscribe any required endpoints to this SNS topic so that these endpoints can receive notification.
- E. Use AWS Trusted Advisor and its security evaluations for the root account. Configure an Amazon EventBridge event rule that is invoked by the Trusted Advisor API. Configure the rule to target an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe any required endpoints to the SNS topic so that these endpoints can receive notification.

Answer: A,C

Explanation:
To receive near-real-time notifications of AWS account root user sign-ins, the most effective solutions involve the use of AWS CloudTrail logs, Amazon CloudWatch Logs, and Amazon EventBridge.
Solution C involves configuring AWS CloudTrail to send logs to Amazon CloudWatch Logs and then setting up a CloudWatch Logs metric filter to detect successful root account logins. When such logins are detected, a CloudWatch alarm can be configured to trigger and notify an Amazon Simple Notification Service (Amazon SNS) topic, which in turn can send notifications to the required endpoints. This solution provides an efficient way to monitor and alert on root account usage without requiring custom parsing or handling of log data.
Solution E uses Amazon EventBridge to monitor for specific AWS API calls, such as SignIn events that indicate a successful root account login. By configuring an EventBridge rule to trigger on these events, notifications can be sent directly to an SNS topic, which then distributes the alerts to the necessary endpoints. This approach leverages native AWS event patterns and provides a streamlined mechanism for detecting and alerting on root account activity.
Both solutions offer automation, scalability, and the ability to integrate with other AWS services, ensuring that stakeholders are promptly alerted to critical security events involving the root user.

NEW QUESTION # 59
A company stores sensitive documents in Amazon S3 by using server-side encryption with an IAM Key Management Service (IAM KMS) CMK. A new requirement mandates that the CMK that is used for these documents can be used only for S3 actions.
Which statement should the company add to the key policy to meet this requirement?

- A.
```
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "kms:*",
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "kms:CallerAccount": "s3.amazonaws.com"
    }
  }
}
```
- B.
```
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:*",
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "kms:ViaService": "kms.*amazonaws.com"
    }
  }
}
```

Answer: A

NEW QUESTION # 60
A company is deploying an Amazon EC2-based application. The application will include a custom health-checking component that produces health status data in JSON format. A Security Engineer must implement a secure solution to monitor application availability in near-real time by analyzing the hearth status data.
Which approach should the Security Engineer use?

- A. Use Amazon CloudWatch monitoring to capture Amazon EC2 and networking metrics Visualize metrics using Amazon CloudWatch dashboards.
- B. Write the status data directly to a public Amazon S3 bucket from the health-checking component Configure S3 events to invoke an IAM Lambda function that analyzes the data
- C. Run the Amazon Kinesis Agent to write the status data to Amazon Kinesis Data Firehose Store the streaming data from Kinesis Data Firehose in Amazon Redshift. (hen run a script on the pool data and analyze the data in Amazon Redshift
- D. Generate events from the health-checking component and send them to Amazon CloudWatch Events. Include the status data as event payloads. Use CloudWatch Events rules to invoke an IAM Lambda function that analyzes the data.

Answer: A

Explanation:
Amazon CloudWatch monitoring is a service that collects and tracks metrics from AWS resources and applications, and provides visualization tools and alarms to monitor performance and availability1. The health status data in JSON format can be sent to CloudWatch as custom metrics2, and then displayed in CloudWatch dashboards3. The other options are either inefficient or insecure for monitoring application availability in near-real time.

NEW QUESTION # 61
A company wants to implement host-based security for Amazon EC2 instances and containers in Amazon Elastic Container Registry (Amazon ECR). The company has deployed AWS Systems Manager Agent (SSM Agent) on the EC2 instances. All the company's AWS accounts are in one organization in AWS Organizations. The company will analyze the workloads for software vulnerabilities and unintended network exposure. The company will push any findings to AWS Security Hub. which the company has configured for the organization.
The company must deploy the solution to all member accounts, including pew accounts, automatically. When new workloads come

online, the solution must scan the workloads.
Which solution will meet these requirements?

- A. Use SCPs to configure scanning of EC2 instances and ECR containers for all accounts in the organization.
- B. Configure a delegated administrator for Amazon Inspector for the organization. Configure automatic scanning for new member accounts.
- C. Configure a delegated administrator for Amazon GuardDuty for the organization. Create an Amazon EventBridge rule to initiate analysis of ECR containers
- D. Configure a delegated administrator for Amazon Inspector for the organization. Create an AWS Config rule to initiate analysis of ECR containers

Answer: B

Explanation:
To implement host-based security for Amazon EC2 instances and containers in Amazon ECR with minimal operational overhead and ensure automatic deployment and scanning for new workloads, the recommended solution is to configure a delegated administrator for Amazon Inspector within the AWS Organizations structure. By enabling Amazon Inspector for the organization and configuring it to automatically scan new member accounts, the company can ensure that all EC2 instances and ECR containers are analyzed for software vulnerabilities and unintended network exposure. Amazon Inspector will automatically assess the workloads and push findings to AWS Security Hub, providing centralized security monitoring and compliance checking. This approach ensures that as new accounts or workloads are added, they are automatically included in the security assessments, maintaining a consistent security posture across the organization with minimal manual intervention.

NEW QUESTION # 62
.....

lb.abcbbk.com, www.stes.tyc.edu.tw, knowyourmeme.com, 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, d2.ilc.edu.tw, vibelearny.com, www.stes.tyc.edu.tw, bbs.t-firefly.com, Disposable vapes

DOWNLOAD the newest Easy4Engine SCS-C02 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1KVyB6N_MVxKolc0srgd8pIqfCc5m8eP2