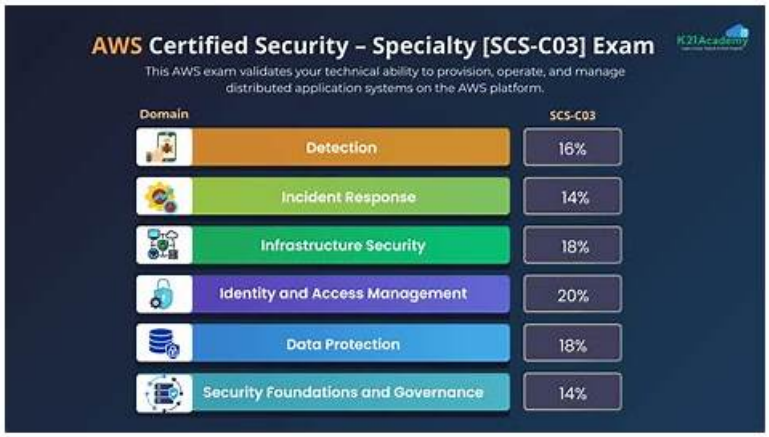
SCS-C03考題資源 & SCS-C03認證題庫



此外，這些Fast2test SCS-C03考試題庫的部分內容現在是免費的：https://drive.google.com/open?id=12rI_dOVD6atX0dd3pftxrjsc2-OW22G2

如果你正在準備 SCS-C03 考試，為 SCS-C03 認證做最後衝刺，又苦於沒有絕對權威的考試真題模擬。很多考生現在都用 Amazon SCS-C03 考題作為參加SCS-C03 考試最快捷，最信任的方式。擺正好心態，認真閱讀准備好的 SCS-C03 考題，考試時心中不要慌，任何一場考試，都是與考生在進行心理戰的准備，遇到難的題目先不要去管，調整好心態准備應戰下一條題目。加上之前准備充足獲取 SCS-C03 認證應該是沒有問題的。

Amazon SCS-C03 考試大綱：

主題	簡介
主題 1	• Detection: This domain covers identifying and monitoring security events, threats, and vulnerabilities in AWS through logging, monitoring, and alerting mechanisms to detect anomalies and unauthorized access.
主題 2	• 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.
主題 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.

>> SCS-C03考題資源 <<

Amazon SCS-C03考題資源和Fast2test - 保證認證成功，簡便的培訓方式

Fast2test是一個專門為IT認證考試人員提供培訓工具的專業網站，也是一個能幫你通過SCS-C03考試很好的選擇。Fast2test會為SCS-C03考試提供一些相關的考試材料，來為你們這些IT專業人士提供鞏固學習的機會。Fast2test會為參加SCS-C03認證考試的人員提供一切最新的他們想要的準確的考試練習題和答案。

最新的 AWS Certified Specialty SCS-C03 免費考試真題 (Q161-Q166):

問題 #161
A company has configured an organization in AWS Organizations for its AWS accounts. AWS CloudTrail is enabled in all AWS Regions.
A security engineer must implement a solution toprevent CloudTrail from being disabled.
Which solution will meet this requirement?

- A. Enable server-side encryption with AWS KMS keys (SSE-KMS) for CloudTrail logs. Create a KMS key. Attach a policy to the key to prevent decryption of the logs.

- B. Create IAM policies for all the company's users to prevent the users from performing the DescribeTrails action and the GetTrailStatus action.
- C. Create a service control policy (SCP) that includes an explicitDenyrule for the cloudtrail:StopLogging action and the cloudtrail:DeleteTrail action. Attach the SCP to the root OU.
- D. Enable CloudTrail log file integrity validation from the organization's management account.

答案：C

解題說明：
AWS CloudTrail is a foundational security service that records API activity and account events. According to the AWS Certified Security - Specialty Official Study Guide,the only way to centrally and reliably prevent CloudTrail from being disabled across multiple AWS accounts is by using AWS Organizations service control policies (SCPs).
SCPs define themaximum available permissionsfor all accounts in an organization or organizational unit.
By creating an SCP with an explicitDenyfor the cloudtrail:StopLogging and cloudtrail:DeleteTrail actions and attaching it to theroot OU, the security engineer ensures thatno principal in any member account- including administrators-can stop or delete CloudTrail trails. Explicit denies in SCPs cannot be overridden by IAM permissions.
Option A is incorrect because log file integrity validation only detects tampering after logs are delivered and does not prevent CloudTrail from being disabled. Option B protects log data at rest but does not prevent trail deletion or logging suspension. Option D removes read-only permissions and does not affect the ability to stop or delete CloudTrail.
AWS documentation explicitly states thatSCPs are the recommended mechanism to enforce mandatory security controls such as CloudTrail logging across an organization, making this the correct and most secure solution.
* AWS Certified Security - Specialty Official Study Guide
* AWS Organizations SCP Documentation
* AWS CloudTrail Security Best Practices

問題 #162
A company's security engineer is designing an isolation procedure for Amazon EC2 instances as part of an incident response plan. The security engineer needs to isolate a target instance to block any traffic to and from the target instance, except for traffic from the company's forensics team. Each of the company's EC2 instances has its own dedicated security group. The EC2 instances are deployed in subnets of a VPC. A subnet can contain multiple instances.
The security engineer is testing the procedure for EC2 isolation and opens an SSH session to the target instance. The procedure starts to simulate access to the target instance by an attacker.
The security engineer removes the existing security group rules and adds security group rules to give the forensics team access to the target instance on port 22.
After these changes, the security engineer notices that the SSH connection is still active and usable. When the security engineer runs a ping command to the public IP address of the target instance, the ping command is blocked.
What should the security engineer do to isolate the target instance?

- A. Create a network ACL that is associated with the target instance's subnet. Add a rule at the top of the inbound rule set to deny all traffic from 0.0.0.0/0. Add a rule at the top of the outbound rule set to deny all traffic to 0.0.0.0/0.
- B. Create an AWS Systems Manager document that adds a host-level firewall rule to block all inbound traffic and outbound traffic. Run the document on the target instance.
- C. Remove the port 22 security group rule. Attach an instance role policy that allows AWS Systems Manager Session Manager connections so that the forensics team can access the target instance.
- D. Add an inbound rule to the security group to allow traffic from 0.0.0.0/0 for all ports. Add an outbound rule to the security group to allow traffic to 0.0.0.0/0 for all ports. Then immediately delete these rules.

答案：A

解題說明：
Amazon EC2 security groups are stateful, meaning that once a connection is established, return traffic is automatically allowed, even if the inbound rule that originally permitted the connection is later removed. According to the AWS Certified Security - Specialty Official Study Guide and Amazon EC2 security documentation, existing connections are not terminated when security group rules change. This explains why the SSH session remains active even after the security group rules were modified, while new traffic such as ICMP ping is blocked.
To immediately and fully isolate an EC2 instance during an incident response scenario, AWS recommends using stateless network controls. Amazon VPC network ACLs (NACLs) are stateless, which means that every packet is evaluated against the ACL rules regardless of whether the traffic is part of an existing connection. When a deny rule is added, all traffic is immediately blocked, including active sessions.
By creating a network ACL and associating it with the subnet that contains the target instance, and by adding explicit deny rules with

the lowest rule numbers for both inbound and outbound traffic, the security engineer ensures that all network communication to and from the instance is immediately interrupted. This approach satisfies the requirement to isolate the instance while preserving its runtime state and memory for forensic analysis.
Other options fail to meet the requirement because security group modifications do not terminate existing sessions, Systems Manager does not enforce network isolation, and host-level firewall changes require instance-level access and do not provide immediate, network-enforced isolation.

問題 #163
A company runs an application on a fleet of Amazon EC2 instances. The application is accessible to users around the world. The company associates an AWS WAF web ACL with an Application Load Balancer (ALB) that routes traffic to the EC2 instances.
A security engineer is investigating a sudden increase in traffic to the application. The security engineer discovers a significant amount of potentially malicious requests coming from hundreds of IP addresses in two countries. The security engineer wants to quickly limit the potentially malicious requests. The security engineer does not want to prevent legitimate users from accessing the application.
Which solution will meet these requirements?

- A. Edit the ALB security group to include a geographical match rule to block all incoming traffic from the two countries.
- B. Use AWS WAF to implement a rate-based rule for all incoming requests.
- C. Use AWS WAF to implement a geographical match rule to block all incoming traffic from the two countries.
- D. Add deny rules to the ALB security group that prohibit incoming requests from the IP addresses.

答案：B

解題說明：
A rate-based rule in AWS WAF is designed to quickly mitigate spikes and potential layer 7 floods bytracking request rates per originating IPand temporarily blocking (or counting/challenging, depending on configuration) IPs that exceed a defined threshold within a 5-minute rolling window. In this scenario, the malicious traffic is distributed acrosshundreds of IPsin two countries, and the application still needs to remain available globally for legitimate users. A rate-based rule provides fast, targeted throttling that reduces abusive request patterns without permanently blocking entire geographies. This aligns with "quickly limit" while minimizing collateral impact.
Blocking both countries with a geo match rule (Option B) would likely block legitimate users located in those countries, which violates the requirement. Security groups (Options C and D) cannot natively enforcegeographicfiltering, and they are not well suited for large, rapidly changing sets of public source IPs at the application layer. Additionally, WAF operates at layer 7 with richer matching (rate limiting, URI/header patterns, bot controls), which is the appropriate control point when the ALB already has a web ACL associated. Therefore, implementing an AWS WAFrate-basedrule is the most effective and least disruptive immediate mitigation.

問題 #164
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 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.
- B. 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.
- C. 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.
- D. 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.

答案：A

解題說明：
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

問題 #165
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 and configure AWS Config. Deploy the Operational Best Practices for PCI DSS conformance pack in AWS Config. Use AWS Config to generate the report.
- B. Enable AWS Security Hub. Enable the Security Hub PCI DSS security standard. Use the AWS Management Console to download the report from the security standard.
- C. Create an AWS Audit Manager assessment that uses the AWS managed PCI DSS v4.0 standard framework. Add all evidence to the assessment. Generate the report in Audit Manager for download.
- D. Enable AWS Trusted Advisor. Configure all the Trusted Advisor checks. Manually map the checks against the PCI DSS v4.0 standard to generate the report.

答案：C

解題說明：
AWS Audit Manager is specifically designed to help organizations continuously audit their AWS usage against compliance frameworks and generate audit-ready reports. According to AWS Certified Security - Specialty documentation, Audit Manager includes AWS managed frameworks for compliance standards, including PCI DSS v4.0.
Audit Manager automatically collects evidence from AWS services such as API Gateway, Lambda, RDS, CloudTrail, and Config, and maps the evidence directly to PCI DSS controls. Importantly, Audit Manager allows compliance teams to upload and attach manual evidence, which is a key requirement in this scenario.
Option C provides visibility into control status but does not support adding manual evidence. Option B evaluates configuration compliance but does not generate formal compliance reports. Option A requires extensive manual effort and is not aligned with PCI reporting workflows.
AWS documentation positions Audit Manager as the authoritative service for compliance reporting and audit evidence management.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
AWS Audit Manager PCI DSS Framework
AWS Compliance Reporting Best Practices

問題 #166
.....

- SCS-C03題庫資料 □ SCS-C03認證題庫 □ 最新SCS-C03題庫資源 □ 透過⇛ www.vcesoft.com ⇚輕鬆獲取（ SCS-C03 ）免費下載SCS-C03考試資訊
- 已驗證的SCS-C03考題資源 |第一次嘗試輕鬆學習並通過考試和完美的Amazon AWS Certified Security - Specialty □ 透過➠ www.newdumpspdf.com □輕鬆獲取「 SCS-C03 」免費下載免費下載SCS-C03考題
- 全面覆蓋的SCS-C03考題資源 |第一次嘗試輕鬆學習和通過考試和優質的SCS-C03：AWS Certified Security - Specialty □ ➠ www.newdumpspdf.com □上的「 SCS-C03 」免費下載只需搜尋SCS-C03考試指南
- SCS-C03最新題庫資源 □ SCS-C03考題套裝 □ SCS-C03考試資訊 □ 請在➥ www.newdumpspdf.com □網站上免費下載➥ SCS-C03 □題庫SCS-C03熱門考古題
- SCS-C03考題套裝 □ 最新SCS-C03考古題 ❣ 免費下載SCS-C03考題 □ 到▷ www.pdfexamdumps.com ◁搜索☀ SCS-C03 □☀□輕鬆取得免費下載SCS-C03考題套裝
- 已驗證的SCS-C03考題資源 |第一次嘗試輕鬆學習並通過考試和完美的Amazon AWS Certified Security - Specialty □ 立即打開☀ www.newdumpspdf.com □☀□並搜索（ SCS-C03 ）以獲取免費下載SCS-C03更新
- SCS-C03熱門考古題 □ 最新SCS-C03題庫資源 □ SCS-C03在線考題 ✌ 在□ www.pdfexamdumps.com □網站上免費搜索□ SCS-C03 □題庫SCS-C03考試內容
- 信賴可靠SCS-C03考題資源是最快捷的通過方式AWS Certified Security - Specialty □ 進入➡ www.newdumpspdf.com □□□搜尋▸ SCS-C03 ◂免費下載SCS-C03考題套裝
- SCS-C03考題套裝 □ 最新SCS-C03考古題 □ SCS-C03更新 □ 立即到“www.newdumpspdf.com”上搜索➤ SCS-C03 □以獲取免費下載SCS-C03考試內容
- bbs.t-firefly.com, hhi.instructure.com, www.xiaokedou21.com, www.stes.tyc.edu.tw, www.ted.com, myportal.utt.edu.tt, k12.instructure.com, rupeebazar.com, Disposable vapes

BONUS!!! 免費下載Fast2test SCS-C03考試題庫的完整版：https://drive.google.com/open?id=12rI_dOVD6atX0dd3pftxrjsc2-OW22G2