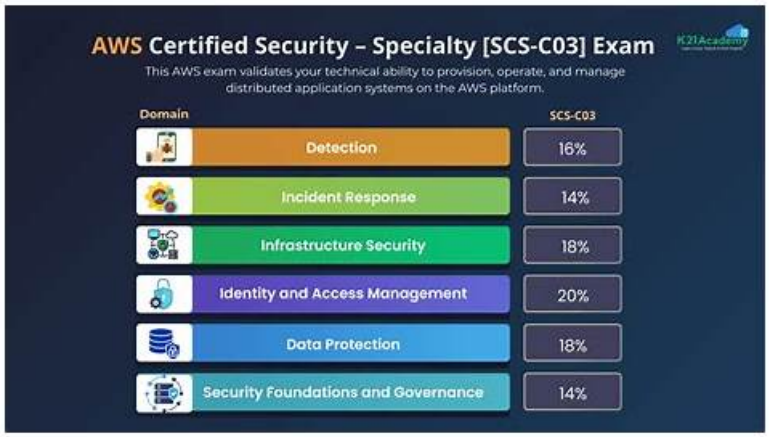
Amazon SCS-C03関連合格問題 & SCS-C03受験資格



P.S.ShikenPASSがGoogle Driveで共有している無料の2026 Amazon SCS-C03ダンプ：https://drive.google.com/open?id=1iVSAJgImlZ1aNl7kP3ClOz2ATYEJc5J3

ShikenPASSのAmazon　SCS-C03問題集は専門家たちが数年間で過去のデータから分析して作成されて、試験にカバーする範囲は広くて、受験生の皆様のお金と時間を節約します。我々SCS-C03問題集の通過率は高いので、90%の合格率を保証します。あなたは弊社の高品質Amazon　SCS-C03試験資料を利用して、一回に試験に合格します。

Amazon SCS-C03 認定試験の出題範囲：

トピック	出題範囲
トピック 1	• インフラストラクチャセキュリティ：このドメインは、セキュアなアーキテクチャ、保護メカニズム、および強化された構成を通じて、ネットワーク、コンピューティングリソース、エッジサービスを含むAWSインフラストラクチャのセキュリティ確保に重点を置いています。
トピック 2	• インシデント対応：この領域では、自動化および手動による戦略、封じ込め、フォレンジック分析、復旧手順を通じてセキュリティインシデントに対応し、影響を最小限に抑え、業務を復旧させることを扱います。
トピック 3	• データ保護：この分野は、暗号化、鍵管理、データ分類、安全な保管、バックアップメカニズムを通じて、保存時および転送時のデータを保護することに重点を置いています。
トピック 4	• IDおよびアクセス管理：この領域は、ユーザーID管理、ロールベースアクセス、フェデレーション、最小権限の原則の実装を通じて、認証と認可を制御することを扱います。
トピック 5	• セキュリティの基盤とガバナンス：このドメインでは、AWS環境におけるポリシー、コンプライアンスフレームワーク、リスク管理、セキュリティ自動化、監査手順など、セキュリティの基盤となる実践方法を取り上げます。

>> Amazon SCS-C03関連合格問題 <<

ユニークなSCS-C03関連合格問題試験-試験の準備方法-効率的なSCS-C03受験資格

ShikenPASSのAmazonのSCS-C03試験トレーニング資料はあなたに時間とエネルギーを節約させます。あなたが何ヶ月でやる必要があることを我々はやってさしあげましたから。あなたがするべきことは、ShikenPASSのAmazonのSCS-C03試験トレーニング資料に受かるのです。あなた自身のために、証明書をもらいます。ShikenPASS はあなたに必要とした知識と経験を提供して、AmazonのSCS-C03試験の目標を作ってあげました。

ShikenPASSを利用したら、試験に合格しないことは絶対ないです。

Amazon AWS Certified Security - Specialty 認定 SCS-C03 試験問題 (Q98-Q103):

質問 # 98
A security engineer configured VPC Flow Logs to publish to Amazon CloudWatch Logs. After 10 minutes, no logs appear. The issue is isolated to the IAM role associated with VPC Flow Logs.
What could be the reason?

- A. The engineer cannot assume the role.
- B. logs:GetLogEvents is missing.
- C. The vpc-flow-logs.amazonaws.com principal cannot assume the role.
- D. The role cannot tag the log stream.

正解：C

解説：
VPC Flow Logs require an IAM role that CloudWatch Logs can use to publish flow log records. AWS documentation and AWS Certified Security - Specialty materials explain that the VPC Flow Logs service must be able to assume the IAM role through its trust policy. The trust relationship must include the service principal vpc-flow-logs.amazonaws.com. If the trust policy does not allow this principal to assume the role, flow logs cannot be delivered and no records will appear in the CloudWatch Logs log group even when traffic exists. logs:GetLogEvents is not required for delivery; it is used for reading logs. The security engineer's ability to assume the role is not relevant because the service, not the engineer, assumes it. Tagging permissions are not required for basic log delivery. Therefore, the most likely cause is an incorrect trust policy that prevents the VPC Flow Logs service principal from assuming the role.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
Amazon VPC Flow Logs IAM Role Requirements
IAM Trust Policies for AWS Services

質問 # 99
A development team is creating an open source toolset to manage a company's software as a service (SaaS) application. The company stores the code in a public repository so that anyone can view and download the toolset's code. The company discovers that the code contains an IAM access key and secret key that provide access to internal resources in the company ' s AWS environment. A security engineer must implement a solution to identify whether unauthorized usage of the exposed credentials has occurred. The solution also must prevent any additional usage of the exposed credentials.
Which combination of steps will meet these requirements? (Select TWO.)

- A. Create a new IAM access key and secret key for the user whose credentials were exposed.
- B. Create a rule in Amazon GuardDuty to block the access key in the source code from being used.
- C. Deactivate the exposed IAM access key from the user ' s IAM account.
- D. Use AWS Identity and Access Management Access Analyzer to determine which resources the exposed credentials accessed and who used them.
- E. Generate an IAM credential report. Check the report to determine when the user that owns the access key last logged in.

正解：C、E

解説：
The immediate containment step for exposed access keys is todisable (deactivate) the compromised IAM access key(Option B). This prevents any further use of the leaked credentials, which is essential once secrets are publicly exposed. Creating a new key (Option D) may be part of recovery later, but it does not stop abuse of the already exposed key unless the exposed key is first deactivated.
To determine whether the credentials were used, you need evidence of access activity. Among the provided options, the best fit is generating and reviewing theIAM credential report(Option E). The report includes metadata such as access key status and "last used" style details that help triage whether the user's credentials have been exercised recently. While deeper investigation would typically rely on CloudTrail "AccessKeyId" searches, the credential report is a quick AWS-native step aligned to the answer choices.
Option A is not correct: IAM Access Analyzer helps identify external access paths to resources and validate policies; it does not provide a definitive history of what a specific access key did. Option C is not a GuardDuty capability-GuardDuty generates findings;

it does not "block" a specific access key. Therefore, deactivating the key and using credential reporting to assess recent usage best matches the requirements.

質問 # 100
A company runs an internet-accessible application on several Amazon EC2 instances that run Windows Server. The company used an instance profile to configure the EC2 instances. A security team currently accesses the VPC that hosts the EC2 instances by using an AWS Site-to- Site VPN tunnel from an on-premises office.
The security team issues a policy that requires all external access to the VPC to be blocked in the event of a security incident. However, during an incident, the security team must be able to access the EC2 instances to obtain forensic information on the instances.
Which solution will meet these requirements?

- A. Install EC2 Instance Connect on the EC2 instances. Configure the instances to permit access to the ec2-instance-connect command user. Use the AWS Management Console to connect to the EC2 instances.
- B. Install EC2 Instance Connect on the EC2 instances. Update the IAM policy for the IAM role to grant the required permissions. Use the AWS CLI to open a tunnel to connect to the instances.
- C. Create an EC2 Instance Connect endpoint in the VPC. Configure an appropriate security group to allow access between the EC2 instances and the endpoint. Use the AWS Management Console to connect to the EC2 instances.
- D. Create an EC2 Instance Connect endpoint in the VPC. Configure an appropriate security group to allow access between the EC2 instances and the endpoint. Use the AWS CLI to open a tunnel to connect to the instances.

正解：C

解説：
EC2 Instance Connect endpoints provide secure, private connectivity to EC2 instances without requiring public IP addresses, inbound internet access, or VPN connectivity. According to AWS Certified Security - Specialty documentation, Instance Connect endpoints are designed specifically for incident response and secure administrative access scenarios.
By deploying an EC2 Instance Connect endpoint in the VPC, the security team can block all external network access while still maintaining controlled access to EC2 instances through the AWS Management Console. The endpoint uses AWS-managed infrastructure and private connectivity, and access is authorized using IAM policies and instance profiles.
Options A and B rely on direct EC2 Instance Connect installation and network paths that may still depend on external access.
Option C is incorrect because tunneling is not required when using the console-based Instance Connect endpoint.
This solution enables forensic access during incidents without reopening external network paths, aligning with AWS incident response best practices.

質問 # 101
A company's security engineer receives an alert that indicates that an unexpected principal is accessing a company-owned Amazon Simple Queue Service (Amazon SQS) queue. All the company's accounts are within an organization in AWS Organizations. The security engineer must implement a mitigation solution that minimizes compliance violations and investment in tools that are outside of AWS. What should the security engineer do to meet these requirements?

- A. In all the VPCs in the organization, adjust the network ACLs to only accept inbound traffic from the CIDR blocks of all the VPCs in the organization. Attach the network ACLs to all the subnets in all the VPCs in the organization.
- B. Create security groups that only accept inbound traffic from the CIDR blocks of all the VPCs in the organization. Attach the security groups to all the SQS queues in all the VPCs in the organization.
- C. Use a cloud access security broker (CASB) to maintain a list of managed resources. Configure the CASB to check the API and console access against that list on a web proxy.
- D. Create interface VPC endpoints for Amazon SQS in all the VPCs in the organization. Set the aws:SourceVpce condition to the VPC endpoint identifier on the SQS policy. Add the aws:PrincipalOrgId condition to the VPC endpoint policy.

正解：D

解説：
Amazon SQS is an AWS-managed service and does not operate within customer VPCs.
Therefore, security groups and network ACLs cannot be used to control access to SQS, making options A and B invalid.
According to AWS Certified Security - Specialty documentation, the recommended approach to securely access AWS services from within a VPC is through interface VPC endpoints (AWS PrivateLink).
By creating interface VPC endpoints for Amazon SQS, the company ensures that traffic to SQS stays within the AWS network and does not traverse the public internet. Adding an SQS resource policy with the aws:SourceVpce condition restricts access so that

only requests originating from the specified VPC endpoint are allowed. Additionally, using the aws:PrincipalOrgId condition ensures that only principals belonging to the same AWS Organization can access the queue.
Option D introduces an external tool, increasing cost and compliance complexity, which directly violates the requirement to minimize investment outside AWS.
AWS documentation clearly identifies VPC endpoints combined with IAM condition keys as a best practice for securing service access in multi-account environments.

質問 # 102
A company runs ECS services behind an internet-facing ALB that is the origin for CloudFront. An AWS WAF web ACL is associated with CloudFront, but clients can bypass it by accessing the ALB directly. Which solution will prevent direct access to the ALB?

- A. Restrict ALB listener rules to CloudFront IP ranges.
- B. Require a custom header from CloudFront and validate it at the ALB.
- C. Use AWS PrivateLink with the ALB.
- D. Replace the ALB with an internal ALB.

正解：B

解説：
AWS best practices recommend using a shared secret header between CloudFront and ALB origins to prevent direct access.
CloudFront injects a custom header, and the ALB listener rules validate its presence.
IP-based controls are brittle due to CloudFront IP changes. PrivateLink and internal ALBs are not supported as CloudFront origins.
Header validation is the most reliable and widely recommended pattern.

質問 # 103
.....

- SCS-C03認定テキスト □ SCS-C03全真模擬試験 □ SCS-C03復習問題集 □ ➤ SCS-C03 □を無料でダウンロード“www.it-passports.com”ウェブサイトを入力するだけSCS-C03コンポーネント
- adhyayon.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, 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, ycs.instructure.com, bicyclebuysell.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, 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, www.sf2.net, Disposable vapes

さらに、ShikenPASS SCS-C03ダンプの一部が現在無料で提供されています：https://drive.google.com/open?id=1iVSAJgImlZ1aNl7kP3ClOz2ATYEJc5J3