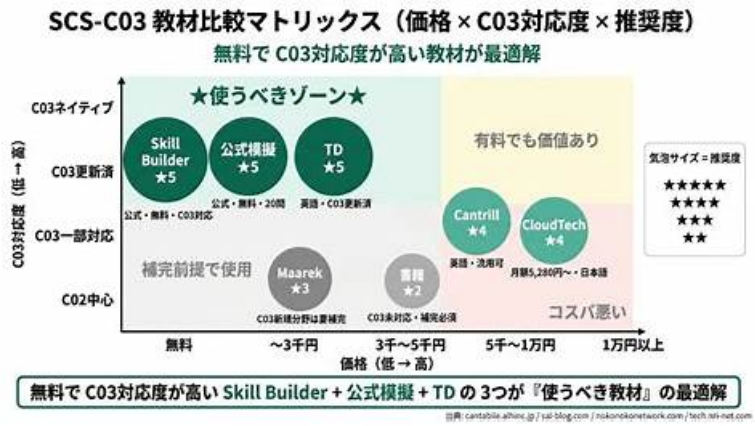
SCS-C03テストサンプル問題、SCS-C03無料過去問



最短時間でSCS-C03試験に合格し、関連する認定資格を取得する場合、当社のSCS-C03トレーニング資料を選択することは、すべての人々の利益になります。あなたのSCS-C03試験に合格し、想像を超える最短時間で関連する認定資格を取得することが非常に簡単になることを確認できます。ウェブからSCS-C03認定トレーニング資料の手順を知ることができます。また、SCS-C03試験問題のデモを無料でダウンロードして、支払い前に確認することもできます。

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	• 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 3	• 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。

>> SCS-C03テストサンプル問題 <<

認定するSCS-C03テストサンプル問題 & 合格スムーズSCS-C03無料過去問 | 高品質なSCS-C03参考資料 AWS Certified Security - Specialty

長年のマーケティングを通じて、当社のSCS-C03最新の認定ガイドは多くのお客様のサポートを獲得しています。最も明白なデータは、当社の製品が毎年徐々に増加していることであり、当社の製品開発のおかげでこのような大きな成功を達成するための大きな努力です。まず、資料の更新を研究する上で非常に良い仕事をしました。さらに、SCS-C03の実際のSCS-C03学習ガイド教材の品質は、教師によって厳密に管理されています。だから、私たちは正しい選択だと信じています。SCS-C03学習教材について質問がある場合は、ご相談ください。

Amazon AWS Certified Security - Specialty 認定 SCS-C03 試験問題 (Q43-Q48):

質問 # 43
A company uses AWS Organizations and has an SCP at the root that prevents sharing resources with external accounts. The

company now needs to allow only the marketing account to share resources externally while preventing all other accounts from doing so. All accounts are in the same OU. Which solution will meet these requirements?

- A. Edit the SCP to include an Allow statement for the marketing account.
- B. Create a new SCP in the marketing account to explicitly allow sharing.
- C. Use a permissions boundary in the marketing account.
- D. Edit the existing SCP to add a condition that excludes the marketing account.

正解：D

解説：
Service control policies (SCPs) define the maximum available permissions for accounts and are evaluated as guardrails. AWS Certified Security - Specialty documentation states SCPs are typically used to apply organization-wide restrictions, and exceptions are commonly handled by using conditions (for example, excluding specific accounts) or by structuring OUs differently.
Because all accounts are in the same OU and the company must continue blocking external sharing for everyone except one account, modifying the existing SCP to exclude the marketing account is the most direct solution. An SCP attached at the root affects all accounts unless conditions narrow its scope. Adding a condition that excludes the marketing account allows that account to retain the ability to share resources externally while the SCP continues to block sharing for other accounts. Option A is not feasible because account-level SCPs cannot override a deny applied by a parent SCP; explicit denies always win. Option C misunderstands SCP behavior because SCPs do not grant permissions; they only limit. Option D is an IAM control that cannot override an organization-level deny. Therefore, the only secure, scalable option is to modify the existing SCP with an exception condition for the marketing account.

質問 # 44
A company's application team needs a new AWS Key Management Service (AWS KMS) customer managed key to use with Amazon S3. The company's security policy requires separate keys for different AWS services to limit security exposure. How can a security engineer limit the KMS customer managed key to work with only Amazon S3?

- A. Configure the key policy to allow KMS actions only when the value for the kms:ViaService condition key matches the Amazon S3 service name.
- B. Configure the application's IAM role policy to allow Amazon S3 to perform the iam:PassRole action.
- C. Configure the key policy to allow only Amazon S3 to perform the kms:Encrypt action.
- D. Configure the application's IAM role policy to allow only S3 operations when the operations are combined with the KMS customer managed key.

正解：A

解説：
AWS KMS provides condition keys that can be used to tightly scope how and where a customer managed key can be used. According to the AWS Certified Security - Specialty Study Guide, the kms:ViaService condition key is specifically designed to restrict key usage to requests that originate from a particular AWS service in a specific Region.
By configuring the key policy to allow KMS cryptographic operations only when kms:ViaService equals s3.<region>.amazonaws.com, the security engineer ensures that the key can be used exclusively by Amazon S3. Even if other IAM principals have permissions to use the key, the key cannot be used by other services such as Amazon EC2, Amazon RDS, or AWS Lambda.
Option A is incorrect because AWS services do not assume identities in key policies. Options C and D modify IAM role policies, which do not control how a KMS key is used by AWS services.
AWS documentation clearly states that service-level restrictions must be enforced at the KMS key policy level using condition keys. This approach enforces strong separation of duties and limits blast radius, which aligns with AWS security best practices.

質問 # 45
A company must inventory sensitive data across all Amazon S3 buckets in all accounts from a single security account.

- A. Use Amazon Inspector with Security Hub.
- B. Delegate Amazon Macie and Security Hub administration.
- C. Use Macie with Trusted Advisor.
- D. Use Inspector with Trusted Advisor.

正解：B

解説：
Amazon Macie is the AWS service designed to discover and classify sensitive data in S3. Delegated administration enables centralized visibility across an organization. Security Hub aggregates Macie findings for a single-pane-of-glass view.
Inspector does not scan S3 data. Trusted Advisor is not a sensitive data discovery tool.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
Amazon Macie Multi-Account Architecture

質問 # 46
A company that uses AWS Organizations is using AWS IAM Identity Center to administer access to AWS accounts. A security engineer is creating a custom permission set in IAM Identity Center.
The company will use the permission set across multiple accounts. An AWS managed policy and a customer managed policy are attached to the permission set. The security engineer has full administrative permissions and is operating in the management account.
When the security engineer attempts to assign the permission set to an IAM Identity Center user who has access to multiple accounts, the assignment fails.
What should the security engineer do to resolve this failure?

- A. Remove either the AWS managed policy or the customer managed policy from the permission set. Create a second permission set that includes the removed policy. Apply the permission sets separately to the user.
- B. Evaluate the logic of the AWS managed policy and the customer managed policy. Resolve any policy conflicts in the permission set before deployment.
- C. Create the customer managed policy in every account where the permission set is assigned. Give the customer managed policy the same name and same permissions in each account.
- D. Do not add the new permission set to the user. Instead, edit the user's existing permission set to include the AWS managed policy and the customer managed policy.

正解：C

解説：
AWS IAM Identity Center permission sets that include customer managed policies require those policies to exist in each target account. According to the AWS Certified Security - Specialty Study Guide, customer managed policies are account-scoped and are not automatically propagated across accounts by Identity Center.
When assigning a permission set across multiple accounts, Identity Center attempts to attach the referenced customer managed policy in each account. If the policy does not exist, the assignment fails. Creating the same customer managed policy with identical name and permissions in every target account resolves the issue.
Option B increases complexity. Option C does not address the root cause. Option D violates Identity Center management best practices.
AWS documentation clearly states that customer managed policies must be present in all accounts where permission sets are applied.

質問 # 47
A public subnet contains two Amazon EC2 instances. The subnet has a custom network ACL. A security engineer is designing a solution to improve the subnet security. The solution must allow outbound traffic to an internet service that uses TLS through port 443. The solution also must deny inbound traffic that is destined for MySQL port 3306.
Which network ACL rule set meets these requirements?

- A. Use inbound rule 100 to allow traffic on TCP port 443. Use inbound rule 200 to deny traffic on TCP port 3306. Use outbound rule 100 to allow traffic on TCP port 443.
- B. Use inbound rule 100 to deny traffic on TCP port 3306. Use inbound rule 200 to allow traffic on TCP port 443. Use outbound rule 100 to allow traffic on TCP port 443.
- C. Use inbound rule 100 to deny traffic on TCP port 3306. Use inbound rule 200 to allow traffic on TCP port range 1024-65535. Use outbound rule 100 to allow traffic on TCP port 443.
- D. Use inbound rule 100 to allow traffic on TCP port range 1024-65535. Use inbound rule 200 to deny traffic on TCP port 3306. Use outbound rule 100 to allow traffic on TCP port 443.

正解：C

解説：
Network ACLs arestateless, so you must allow both the outbound request and the inboundreturn traffic. For outbound TLS to an

internet service on TCP443, you need an outbound allow rule permitting destination port
443. The return traffic from the internet service will come back to the instance'sephemeral port(typically in the range 1024-65535) on the inbound path. Therefore, you must allow inbound TCP traffic on the ephemeral port range to support established outbound connections.
At the same time, the requirement is todeny inbound MySQL (TCP 3306). Because NACLs process rules in order (lowest rule number first), placing an explicit deny for port 3306 as a low-numbered inbound rule ensures that traffic destined for MySQL is blocked even if there are broader allow rules later.
Option B does exactly this: it denies inbound TCP 3306 first, then allows inbound ephemeral ports for return traffic, and allows outbound TCP 443. Option A/D incorrectly allow inbound 443 (not needed for outbound- only TLS) and fail to explicitly allow ephemeral return traffic correctly. Option C allows ephemeral inbound first, and then denies 3306 later; while 3306 is not in the ephemeral range, B is the clean, canonical ordering and matches the intended stateless-return-traffic pattern most directly.

質問 # 48
.....