SCS-C02日本語参考、SCS-C02参考書内容

BONUS！！！ PassTest SCS-C02ダンプの一部を無料でダウンロード：https://drive.google.com/open?id=1Xx31NtPvyLiWt8PGzsLgCwtLJlv5UrLR

最新のSCS-C02試験トレントは、対応する教材を同時に含む、近年のすべての資格試験シミュレーション問題をカバーしています。有効なSCS-C02練習資料がないと、遅延の進行、学習効率などのユーザーに不便をもたらす可能性があり、学習成果を減らすことは重要ではありませんでした。これらはユーザーの永続的な学習目標を助長しません。したがって、これらの問題を解決するために、SCS-C02テスト材料は、SCS-C02試験に合格するように特別に設計されています。

Amazon SCS-C02 認定試験の出題範囲:

トピック	出題範囲
トピック 1	• 脅威の検出とインシデント対応: このトピックでは、AWS セキュリティスペシャリストが、インシデント対応計画を作成し、AWS サービスを使用してセキュリティの脅威と異常を検出する専門知識を習得します。侵害されたリソースとワークロードに対応するための効果的な戦略を詳しく調べ、セキュリティインシデントを管理する準備を整えます。これらの概念を習得することは、SCS-C02 試験で評価されるシナリオを処理するために不可欠です。
トピック 2	• 管理とセキュリティガバナンス: このトピックでは、AWS セキュリティスペシャリストが AWS アカウント管理と安全なリソース展開のための一元的な戦略を策定する方法を学びます。これには、認定基準に準拠したガバナンスを実装するために不可欠な、アーキテクチャレビューとコスト分析によるコンプライアンスの評価とセキュリティギャップの特定が含まれます。
トピック 3	• データ保護: AWS セキュリティスペシャリストは、転送中および保存中のデータの機密性と整合性を確保する方法を学びます。トピックには、保存データのライフサイクル管理、認証情報の保護、暗号化キーの管理が含まれます。これらの機能は機密データを安全に管理する上で中心的な役割を果たし、高度なデータ保護戦略に重点を置いた試験を反映しています。

トピック４	• インフラストラクチャセキュリティ:AWS セキュリティスペシャリストを目指す人は、このトピックでエッジサービス、ネットワーク、コンピューティングワークロードのセキュリティコントロールを実装およびトラブルシューティングするためのトレーニングを受けます。AWS インフラストラクチャ全体の回復力の確保とリスクの軽減に重点が置かれています。このセクションは、重要な AWS サービスと環境の保護に重点を置く試験と密接に連携しています。

>> SCS-C02日本語参考 <<

SCS-C02参考書内容、SCS-C02勉強の資料

多くのIT者がAmazonのSCS-C02認定試験を通してIT業界の中で良い就職機会を得たくて、生活水準も向上させたいです。でも多くの人が合格するために大量の時間とエネルギーをかかって、無駄になります。同等の効果は、PassTestは君の貴重な時間とお金を節約するだけでなく１００％の合格率を保証いたします。もし弊社の商品が君にとっては何も役割にならなくて全額で返金いたいます。

Amazon AWS Certified Security - Specialty 認定 SCS-C02 試験問題 (Q128-Q133):

質問 # 128
A security engineer needs to create an Amazon S3 bucket policy to grant least privilege read access to IAM user accounts that are named User=1, User2. and User3. These IAM user accounts are members of the AuthorizedPeople IAM group. The security engineer drafts the following S3 bucket policy:

When the security engineer tries to add the policy to the S3 bucket, the following error message appears:
"Missing required field Principal." The security engineer is adding a Principal element to the policy. The addition must provide read access to only User1. User2, and User3. Which solution meets these requirements?

- A. 

- B. 

- C.


- D.


正解：D

質問 # 129
A security engineer is checking an AWS CloudFormation template for vulnerabilities. The security engineer finds a parameter that has a default value that exposes an application's API key in plaintext. The parameter is referenced several times throughout the template. The security engineer must replace the parameter while maintaining the ability to reference the value in the template. Which solution will meet these requirements in the MOST secure way?

- A. Store the API key value in a new Amazon S3 bucket. In the template, replace all references to the value with {
- B. Store the API key value in AWS Secrets Manager. In the template, replace all references to the value with {{resolve:secretsmanager:MySecretId:SecretString}}.
- C. Store the API key value in Amazon DynamoDB. In the template, replace all references to the value with {{resolve:dynamodb:MyTableName:MyPrimaryKey}}.
- D. Store the API key value as a SecureString parameter in AWS Systems Manager Parameter Store. In the template, replace all references to the value with {{resolve:ssm:MySSMParameterName:I}}.

正解：B

解説：
{resolve:s3:MyBucketName:MyObjectName}}.
Explanation:
The correct answer is B. Store the API key value in AWS Secrets Manager. In the template, replace all references to the value with {{resolve:secretsmanager:MySecretId:SecretString}}.
This answer is correct because AWS Secrets Manager is a service that helps you protect secrets that are needed to access your applications, services, and IT resources. You can store and manage secrets such as database credentials, API keys, and other sensitive data in Secrets Manager. You can also use Secrets Manager to rotate, manage, and retrieve your secrets throughout their lifecycle1. Secrets Manager integrates with AWS CloudFormation, which allows you to reference secrets from your templates using the {{resolve:secretsmanager:...}} syntax2. This way, you can avoid exposing your secrets in plaintext and still use them in your resources.
The other options are incorrect because:
A) Storing the API key value as a SecureString parameter in AWS Systems Manager Parameter Store is not a solution, because AWS CloudFormation does not support references to SecureString parameters. This means that you cannot use the {{resolve:ssm:...}} syntax to retrieve encrypted parameter values from Parameter Store3. You would have to use a custom resource or a Lambda function to decrypt the parameter value, which adds complexity and overhead to your template.
C) Storing the API key value in Amazon DynamoDB is not a solution, because AWS CloudFormation does not support references to DynamoDB items. This means that you cannot use the {{resolve:dynamodb:...}} syntax to retrieve item values from DynamoDB tables4. You would have to use a custom resource or a Lambda function to query the DynamoDB table, which adds complexity and overhead to your template.
D) Storing the API key value in a new Amazon S3 bucket is not a solution, because AWS CloudFormation does not support references to S3 objects. This means that you cannot use the {{resolve:s3:...}} syntax to retrieve object values from S3 buckets5. You would have to use a custom resource or a Lambda function to download the object from S3, which adds complexity and overhead to your template.
Reference:
1: What is AWS Secrets Manager? 2: Referencing AWS Secrets Manager secrets from Parameter Store parameters 3: Using dynamic references to specify template values 4: Amazon DynamoDB 5: Amazon Simple Storage Service (S3)

質問 # 130

A security engineer is troubleshooting an AWS Lambda function that is named MyLambdaFunction. The function is encountering an error when the function attempts to read the objects in an Amazon S3 bucket that is named DOC-EXAMPLE-BUCKET. The S3 bucket has the following bucket policy:

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "lambda.amazonaws.com"
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:lambda:::function:MyLambdaFunction"
        }
    }
}
```


Which change should the security engineer make to the policy to ensure that the Lambda function can read the bucket objects?

- A. Remove the Condition element. Change the Principal element to the following:
  {
  "AWS": "arn "aws" ::: lambda ::: function:MyLambdaFunction"
  }
- B. Change the Resource element to "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*".
- C. Change the Resource element to "arn:aws:lambda:::function:MyLambdaFunction". Change the Principal element to the following:
  {
  "Service": "s3.amazonaws.com"
  }
- D. Change the Action element to the following:
  " s3:GetObject*"
  " s3:GetBucket*"

正解：B

解説：
The correct answer is C. Change the Resource element to "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*".
The reason is that the Resource element in the bucket policy specifies which objects in the bucket are affected by the policy. In this case, the policy only applies to the bucket itself, not the objects inside it. Therefore, the Lambda function cannot access the objects with the s3:GetObject permission. To fix this, the Resource element should include a wildcard (*) to match all objects in the bucket. This way, the policy grants the Lambda function permission to read any object in the bucket.
The other options are incorrect for the following reasons:
* A. Removing the Condition element would not help, because it only restricts access based on the source IP address of the request. The Principal element should not be changed to the Lambda function ARN, because it specifies who is allowed or denied access by the policy. The policy should allow access to any principal ("*") and rely on IAM roles or policies to control access to the Lambda function.
* B. Changing the Action element to include s3:GetBucket* would not help, because it would grant additional permissions that are not needed by the Lambda function, such as s3:GetBucketAcl or s3:
GetBucketPolicy. The s3:GetObject* permission is sufficient for reading objects in the bucket.
* D. Changing the Resource element to the Lambda function ARN would not make sense, because it would mean that the policy applies to the Lambda function itself, not the bucket or its objects. The Principal element should not be changed to s3.amazonaws.com, because it would grant access to any AWS service that uses S3, not just Lambda.

質問 # 131
A company deploys a distributed web application on a fleet of Amazon EC2 instances. The fleet is behind an Application Load Balancer (ALB) that will be configured to terminate the TLS connection. All TLS traffic to the ALB must stay secure, even if the certificate private key is compromised.
How can a security engineer meet this requirement?

- A. Create a TCP listener that uses a custom security policy that allows only cipher suites with perfect forward secrecy (PFS).
- B. Create an HTTPS listener that uses a security policy that uses a cipher suite with perfect forward secrecy (PFS).
- C. Create an HTTPS listener that uses a certificate that is managed by AWS Certificate Manager (ACM).
- D. Create an HTTPS listener that uses the Server Order Preference security feature.

正解：B

質問 # 132
A security engineer is setting up an AWS CloudTrail trail for all regions in an AWS account. For added security, the logs are stored using server-side encryption with AWS KMS-managed keys (SSE-KMS) and have log integrity validation enabled.
While testing the solution, the security engineer discovers that the digest files are readable, but the log files are not. What is the MOST likely cause?

- A. The KMS key policy does not grant the security engineer's 1AM user or rote permissions to decrypt with it.
- B. The log flies fail integrity validation and automatically are marked as unavailable.
- C. The bucket is set up to use server-side encryption with Amazon S3-managed keys (SSE-S3) as the default and does not allow SSE-KMS-encrypted files.
- D. An 1AM policy applicable to the security engineer's 1AM user or role denies access to the "CloudTraiir prefix in the Amazon S3 bucket.

正解：A

解説：
* Understanding the Problem:
* Logs are encrypted with a KMS-managed key (SSE-KMS), and the security engineer can read digest files but not the log files.
* This indicates that the issue lies in permissions related to decryption.
* KMS Key Policy:
* The key policy for the KMS-managed key must explicitly allow the security engineer's IAM user or role thekms:Decryptpermission.
Example Key Policy:
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::<account-id>:user/<security-engineer>"
},
"Action": "kms:Decrypt",
"Resource": "*"
}
]
}
* Verify the IAM Role/Policy:
* Ensure that no conflicting IAM policy denies thekms:Decryptaction for the security engineer's user or role.
* Enable Access to Encrypted Logs:
* Update the KMS key policy to include permissions for reading and decrypting CloudTrail logs.
AWS KMS Key Policy Documentation
Server-Side Encryption with KMS for CloudTrail

質問 # 133
.....

- SCS-C02試験の準備方法｜有難いSCS-C02日本語参考試験｜素敵なAWS Certified Security - Specialty参考書内容 □ 最新▸ SCS-C02 ◂問題集ファイルは（ www.passtest.jp ）にて検索SCS-C02資格問題集
- 最高SCS-C02｜検証するSCS-C02日本語参考試験｜試験の準備方法AWS Certified Security - Specialty参考書内容 □ 最新“ SCS-C02 ”問題集ファイルは ➠ www.goshiken.com □にて検索SCS-C02日本語資格取得
- 実用的なSCS-C02日本語参考 - 合格スムーズSCS-C02参考書内容 | 効果的なSCS-C02勉強の資料 AWS Certified Security - Specialty □ “ www.it-passports.com ”に移動し、 ➡ SCS-C02 □□□を検索して無料でダウンロードしてくださいSCS-C02過去問題
- SCS-C02試験の準備方法｜有難いSCS-C02日本語参考試験｜素敵なAWS Certified Security - Specialty参考書内容 □ ➥ SCS-C02 □の試験問題は☀ www.goshiken.com □☀□で無料配信中SCS-C02日本語試験情報
- 実用的なSCS-C02日本語参考 - 合格スムーズSCS-C02参考書内容 | 効果的なSCS-C02勉強の資料 AWS Certified Security - Specialty □ 「 www.shikenpass.com 」サイトで【 SCS-C02 】の最新問題が使えるSCS-C02日本語資格取得
- 有効なSCS-C02学習問題集、SCS-C02信頼できる学習参考書、 □ ➤ www.goshiken.com □サイトで➠ SCS-C02 □の最新問題が使えるSCS-C02試験時間
- SCS-C02復習解答例 □ SCS-C02必殺問題集 □ SCS-C02受験準備 □ ➥ www.mogiexam.com □を開いて ➡ SCS-C02 □□□を検索し、試験資料を無料でダウンロードしてくださいSCS-C02最新試験情報
- SCS-C02模擬解説集 □ SCS-C02日本語版参考資料 □ SCS-C02模擬解説集 □ URL ➤ www.goshiken.com □をコピーして開き、➽ SCS-C02 □を検索して無料でダウンロードしてくださいSCS-C02最新試験情報
- 最高SCS-C02｜検証するSCS-C02日本語参考試験｜試験の準備方法AWS Certified Security - Specialty参考書内容 □ ⇛ SCS-C02 ⇚を無料でダウンロード□ www.goshiken.com □で検索するだけSCS-C02参考資料
- SCS-C02資格問題集 □ SCS-C02過去問題 □ SCS-C02資格問題集 □ サイト➽ www.goshiken.com □で✔ SCS-C02 □✔□問題集をダウンロードSCS-C02参考資料
- 実用的なSCS-C02日本語参考 - 合格スムーズSCS-C02参考書内容 | 効果的なSCS-C02勉強の資料 AWS Certified Security - Specialty □ ➤ www.topexam.jp □で使える無料オンライン版⇒ SCS-C02 ⇐ の試験問題SCS-C02模擬資料
- 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, www.divephotoguide.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, getwisewithmoney.org, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

無料でクラウドストレージから最新のPassTest SCS-C02 PDFダンプをダウンロードする：https://drive.google.com/open?id=1Xx31NtPvyLiWt8PGzsLgCwtLJlv5UrLR