SCS-C02日本語解説集 & SCS-C02科目対策

無料でクラウドストレージから最新のTech4Exam SCS-C02 PDFダンプをダウンロードする：https://drive.google.com/open?id=191POEhY4VoF_NNyPt-oFKHHR6hh6Aizn

人生は自転車に乗ると似ていて、やめない限り、倒れないから。IT技術職員として、周りの人はAmazon　SCS-C02試験に合格し高い月給を持って、上司からご格別の愛護を賜り更なるジョブプロモーションを期待されますけど、あんたはこういうように所有したいますか。変化を期待したいあなたにAmazon　SCS-C02試験備考資料を提供する権威性のあるTech4Examをお勧めさせていただけませんか。

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	• アイデンティティとアクセス管理: このトピックでは、AWS セキュリティ スペシャリストに、AWS リソースの認証および承認メカニズムを設計、実装、トラブルシューティングするスキルを身につけさせます。この領域では、安全なアイデンティティ管理の実践に重点を置き、認定試験の重要な側面である効果的なアクセス制御に必要な基礎的な能力を扱います。
トピック 3	• 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 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日本語解説集 <<

Amazon SCS-C02科目対策、SCS-C02練習問題

Tech4ExamはAmazon試験問題集を提供するウエブダイトで、ここによく分かります。最もよくて最新で資料を提供いたします。こうして、君は安心でSCS-C02試験の準備を行ってください。弊社の資料を使って、１００％に合格を保証いたします。もし合格しないと、われは全額で返金いたします。

Amazon AWS Certified Security - Specialty 認定 SCS-C02 試験問題 (Q371-Q376):

質問 # 371
A company's network security policy requires encryption for all data in transit. The company must encrypt data that is sent between Amazon EC2 instances and Amazon Elastic Block Store (Amazon EBS) volumes.

- A. Configure Amazon EBS to enable volume encryption with AWS Key Management Service (AWS KMS) for data at rest.
- B. Configure Amazon EC2 to enable TLS encryption with certificates that are stored in AWS Certificate Manager (ACM).
- C. Configure Amazon EC2 to enable encryption in the EC2 network interface properties.
- D. Configure Amazon EBS to enable TLS encryption in the volume configuration properties.

正解：B

解説：
Comprehensive Detailed Explanation with all AWS References
To ensure encryption for all data in transit between EC2 instances and EBS volumes,TLS encryptionmust be implemented. While EBS volume encryption secures data at rest, the requirement here is to secure datain transit.
* TLS Encryption with ACM Certificates:
* AWS Certificate Manager (ACM) simplifies the process of deploying TLS encryption by managing certificates.
* EC2 instances can use these certificates for secure data transmission to EBS.
Reference:AWS TLS Encryption Documentation
Incorrect Options:
A:Encryption in the EC2 network interface properties is not a valid configuration.
B:EBS volume encryption secures data at rest, not in transit.
C:TLS encryption cannot be configured in EBS volume properties.

質問 # 372
A company wants to migrate its static primary domain website to AWS. The company hosts the website and DNS servers internally. The company wants the website to enforce SSL/TLS encryption block IP addresses from outside the United States (US), and take advantage of managed services whenever possible.
Which solution will meet these requirements?

- A. Migrate the website to Amazon S3 Import a public SSL certificate to an Application Load. Balancer with rules to block traffic from outside the US Migrate DNS to Amazon Route 53.
- B. Migrate the website to Amazon EC2 Import a public SSL certificate that is created by AWS Certificate Manager (ACM) to an Application Load Balancer with rules to block traffic from outside the US Update DNS accordingly.
- C. Migrate the website to Amazon S3 Import a public SSL certificate that is created by AWS Certificate Manager (ACM) to Amazon. CloudFront Configure CloudFront to block traffic from outside the US.Migrate DNS to Amazon Route 53.
- D. Migrate the website to Amazon S3. Import a public SSL certificate to Amazon CloudFront Use AWS WAF rules to block traffic from outside the US Update DNS.accordingly

正解：C

解説：
To migrate the static website to AWS and meet the requirements, the following steps are required:
* Migrate the website to Amazon S3, which is a highly scalable and durable object storage service that can host static websites. To do this, create an S3 bucket with the same name as the domain name of the website, enable static website hosting for the bucket, upload the website files to the bucket, and configure the bucket policy to allow public read access to the objects. For more information, see Hosting a static website on Amazon S3.
* Import a public SSL certificate that is created by AWS Certificate Manager (ACM) to Amazon CloudFront, which is a global content delivery network (CDN) service that can improve the performance and security of web applications. To do this, request or import a public SSL certificate for the domain name of the website using ACM, create a CloudFront distribution with the S3 bucket

as the origin, and associate the SSL certificate with the distribution. For more information, see Using alternate domain names and HTTPS.
* Configure CloudFront to block traffic from outside the US, which is one of the requirements. To do this, create a CloudFront web ACL using AWS WAF, which is a web application firewall service that lets you control access to your web applications. In the web ACL, create a rule that uses a geo match condition to block requests that originate from countries other than the US. Associate the web ACL with the CloudFront distribution. For more information, see How AWS WAF works with Amazon CloudFront features.
* Migrate DNS to Amazon Route 53, which is a highly available and scalable cloud DNS service that can route traffic to various AWS services. To do this, register or transfer your domain name to Route 53, create a hosted zone for your domain name, and create an alias record that points your domain name to your CloudFront distribution. For more information, see Routing traffic to an Amazon CloudFront web distribution by using your domain name.
The other options are incorrect because they either do not implement SSL/TLS encryption for the website (A), do not use managed services whenever possible (B), or do not block IP addresses from outside the US .
Verified References:
* https://docs.aws.amazon.com/AmazonS3/latest/userguide/HostingWebsiteOnS3Setup.html
* https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-alternate-domain- names.html
* https://docs.aws.amazon.com/waf/latest/developerguide/waf-cloudfront.html
* https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html

質問 # 373
A company has a legacy application that runs on a single Amazon EC2 instance. A security audit shows that the application has been using an IAM access key within its code to access an Amazon S3 bucket that is named DOC-EXAMPLE-BUCKET1 in the same AWS account. This access key pair has the s3:GetObject permission to all objects in only this S3 bucket. The company takes the application offline because the application is not compliant with the company's security policies for accessing other AWS resources from Amazon EC2.
A security engineer validates that AWS CloudTrail is turned on in all AWS Regions. CloudTrail is sending logs to an S3 bucket that is named DOC-EXAMPLE-BUCKET2. This S3 bucket is in the same AWS account as DOC-EXAMPLE-BUCKET1. However, CloudTrail has not been configured to send logs to Amazon CloudWatch Logs.
The company wants to know if any objects in DOC-EXAMPLE-BUCKET1 were accessed with the IAM access key in the past 60 days. If any objects were accessed, the company wants to know if any of the objects that are text files (.txt extension) contained personally identifiable information (PII).
Which combination of steps should the security engineer take to gather this information? (Choose two.)

- A. Use Amazon CloudWatch Logs Insights to identify any objects in DOC-EXAMPLE-BUCKET1 that contain PII and that were available to the access key.
- B. Use AWS Identity and Access Management Access Analyzer to identify any API calls that used the access key to access objects that contained PII in DOC-EXAMPLE-BUCKET1.
- C. Configure Amazon Macie to identify any objects in DOC-EXAMPLE-BUCKET1 that contain PII and that were available to the access key.
- D. Use Amazon Athena to query the CloudTrail logs in DOC-EXAMPLE-BUCKET2 for any API calls that used the access key to access an object that contained PII.
- E. Use Amazon OpenSearch Service (Amazon Elasticsearch Service) to query the CloudTrail logs in DOC-EXAMPLE-BUCKET2 for API calls that used the access key to access an object that contained PII.

正解：C、D

質問 # 374
A company is running its workloads in a single AWS Region and uses AWS Organizations. A security engineer must implement a solution to prevent users from launching resources in other Regions.
Which solution will meet these requirements with the LEAST operational overhead?

- A. Create an IAM policy that has an aws RequestedRegion condition that allows the desired actions Attach the policy only to the users who are in the designated Region.
- B. Create an IAM policy that has an aws RequestedRegion condition that allows actions only in the designated Region Attach the policy to all users.
- C. Create an I AM policy that has an aws RequestedRegion condition that denies actions that are not in the designated Region Attach the policy to the AWS account in AWS Organizations.
- D. Create an SCP that has an aws RequestedRegion condition that denies actions that are not in the designated Region. Attach the SCP to the AWS account in AWS Organizations.

正解：D

解説：
Explanation
Although you can use a IAM policy to prevent users launching resources in other regions. The best practice is to use SCP when using AWS organizations.
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_general.html

質問 # 375
A company wants to migrate its static primary domain website to AWS. The company hosts the website and DNS servers internally. The company wants the website to enforce SSL/TLS encryption block IP addresses from outside the United States (US), and take advantage of managed services whenever possible.
Which solution will meet these requirements?

- A. Migrate the website to Amazon S3. Import a public SSL certificate to Amazon CloudFront Use AWS WAF rules to block traffic from outside the US Update DNS.
  accordingly
- B. Migrate the website to Amazon S3 Import a public SSL certificate to an Application Load. Balancer with rules to block traffic from outside the US Migrate DNS to Amazon Route 53.
- C. Migrate the website to Amazon S3 Import a public SSL certificate that is created by AWS Certificate Manager (ACM) to Amazon. CloudFront Configure CloudFront to block traffic from outside the US.
  Migrate DNS to Amazon Route 53.
- D. Migrate the website to Amazon EC2 Import a public SSL certificate that is created by AWS Certificate Manager (ACM) to an Application Load Balancer with rules to block traffic from outside the US Update DNS accordingly.

正解：C

解説：
To migrate the static website to AWS and meet the requirements, the following steps are required:
* Migrate the website to Amazon S3, which is a highly scalable and durable object storage service that can host static websites. To do this, create an S3 bucket with the same name as the domain name of the website, enable static website hosting for the bucket, upload the website files to the bucket, and configure the bucket policy to allow public read access to the objects. For more information, see Hosting a static website on Amazon S3.
* Import a public SSL certificate that is created by AWS Certificate Manager (ACM) to Amazon CloudFront, which is a global content delivery network (CDN) service that can improve the performance and security of web applications. To do this, request or import a public SSL certificate for the domain name of the website using ACM, create a CloudFront distribution with the S3 bucket as the origin, and associate the SSL certificate with the distribution. For more information, see Using alternate domain names and HTTPS.
* Configure CloudFront to block traffic from outside the US, which is one of the requirements. To do this, create a CloudFront web ACL using AWS WAF, which is a web application firewall service that lets you control access to your web applications. In the web ACL, create a rule that uses a geo match condition to block requests that originate from countries other than the US. Associate the web ACL with the CloudFront distribution. For more information, see How AWS WAF works with Amazon CloudFront features.
* Migrate DNS to Amazon Route 53, which is a highly available and scalable cloud DNS service that can route traffic to various AWS services. To do this, register or transfer your domain name to Route 53, create a hosted zone for your domain name, and create an alias record that points your domain name to your CloudFront distribution. For more information, see Routing traffic to an Amazon CloudFront web distribution by using your domain name.
The other options are incorrect because they either do not implement SSL/TLS encryption for the website (A), do not use managed services whenever possible (B), or do not block IP addresses from outside the US.
Verified References:
* https://docs.aws.amazon.com/AmazonS3/latest/userguide/HostingWebsiteOnS3Setup.html
* https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-alternate-domain-nam
* https://docs.aws.amazon.com/waf/latest/developerguide/waf-cloudfront.html
* https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html

質問 # 376
.....

変化する地域に対応するには、問題を解決する効率を改善する必要があります。これは、試験に対処するだけでなく、多くの側面を反映しています。 SCS-C02実践教材は、あなたがそれを実現するのに役立ちます。これ

らの時間に敏感な試験の受験者にとって、重要なニュースで構成される高効率のSCS-C02実際のテストは、最高の助けになります。定期的にそれらを練習することによってのみ、あなたはあなたに明らかな進歩が起こったのを見るでしょう。それに、SCS-C02練習教材の利益を待つのではなく、支払い後すぐにダウンロードできるので、今すぐ成功への旅を始めましょう。

SCS-C02科目対策: https://www.tech4exam.com/SCS-C02-pass-shiken.html

- 有効的なSCS-C02日本語解説集 - 合格スムーズSCS-C02科目対策 | ユニークなSCS-C02練習問題 □ 今すぐ《 jp.fast2test.com 》で▶ SCS-C02 ◀を検索して、無料でダウンロードしてくださいSCS-C02復習教材
- SCS-C02最新試験 □ SCS-C02科目対策 🏇 SCS-C02クラムメディア □ （ www.goshiken.com ）サイトで“ SCS-C02 ”の最新問題が使えるSCS-C02最新な問題集
- SCS-C02クラムメディア □ SCS-C02受験記 □ SCS-C02復習時間 □ □ www.it-passports.com □で▹ SCS-C02 ◃を検索し、無料でダウンロードしてくださいSCS-C02資格練習
- SCS-C02受験記 □ SCS-C02関連試験 □ SCS-C02クラムメディア □ 《 SCS-C02 》を無料でダウンロード□ www.goshiken.com □ウェブサイトを入力するだけSCS-C02受験記
- SCS-C02クラムメディア □ SCS-C02資格模擬 □ SCS-C02関連試験 □ 【 www.goshiken.com 】に移動し、□ SCS-C02 □を検索して、無料でダウンロード可能な試験資料を探しますSCS-C02受験体験
- SCS-C02教育資料 □ SCS-C02資格練習 □ SCS-C02学習範囲 □ [www.goshiken.com]サイトで“ SCS-C02 ”の最新問題が使えるSCS-C02関連試験
- SCS-C02復習時間 □ SCS-C02的中合格問題集 □ SCS-C02受験体験 □ URL「 www.it-passports.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受験体験
- SCS-C02日本語版試験解答 □ SCS-C02科目対策 □ SCS-C02日本語版試験解答 □ ウェブサイト☀ www.goshiken.com □☀□を開き、➽ SCS-C02 □を検索して無料でダウンロードしてくださいSCS-C02基礎訓練
- SCS-C02最新試験 □ SCS-C02受験体験 □ SCS-C02テストサンプル問題 □ 《 www.shikenpass.com 》にて限定無料の□ SCS-C02 □問題集をダウンロードせよSCS-C02テストサンプル問題
- 有効的なSCS-C02日本語解説集 - 合格スムーズSCS-C02科目対策 | ユニークなSCS-C02練習問題 □ Open Webサイト➡ www.goshiken.com □□□検索➡ SCS-C02 □□□無料ダウンロードSCS-C02受験記
- SCS-C02試験の準備方法 | 最新のSCS-C02日本語解説集試験 | 高品質なAWS Certified Security - Specialty科目対策 □⇒ www.passtest.jp ⇐に移動し、▹ SCS-C02 ◃を検索して、無料でダウンロード可能な試験資料を探しますSCS-C02復習教材
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.yiqn.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, telegra.ph, 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, Disposable vapes

P.S. Tech4ExamがGoogle Driveで共有している無料かつ新しいSCS-C02ダンプ：https://drive.google.com/open?id=191POEhY4VoF_NNyPt-oFKHHR6hh6Aizn