

# 実用的SCS-C02入門知識 & 資格試験のリーダー & 人気の有るSCS-C02: AWS Certified Security - Specialty



BONUS!!! GoShiken SCS-C02ダンプの一部を無料でダウンロード: <https://drive.google.com/open?id=1dUPhmcU04Mqdv4sQpAh-m8cjbI8wbffp>

もしGoShikenのSCS-C02問題集を利用してからやはりSCS-C02認定試験に失敗すれば、あなたは問題集を購入する費用を全部取り返すことができます。これはまさにGoShikenが受験生の皆さんに与えるコミットメントです。優秀な試験参考書は話すことに依頼することではなく、受験生の皆さんに検証されることに依頼するので、GoShikenの参考資料は時間の試練に耐えることができます。GoShikenは現在の実績を持っているのは受験生の皆さんによって実践を通して得られた結果です。真実かつ信頼性の高いものだからこそ、GoShikenの試験参考書は長い時間にわたってますます人気があるようになっています。

## 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	<ul style="list-style-type: none"><li>Security Logging and Monitoring: This topic prepares AWS Security specialists to design and implement robust monitoring and alerting systems for addressing security events. It emphasizes troubleshooting logging solutions and analyzing logs to enhance threat visibility.</li></ul>
トピック 2	<ul style="list-style-type: none"><li>Identity and Access Management: The topic equips AWS Security specialists with skills to design, implement, and troubleshoot authentication and authorization mechanisms for AWS resources. By emphasizing secure identity management practices, this area addresses foundational competencies required for effective access control, a vital aspect of the certification exam.</li></ul>
トピック 3	<ul style="list-style-type: none"><li>Data Protection: AWS Security specialists learn to ensure data confidentiality and integrity for data in transit and at rest. Topics include lifecycle management of data at rest, credential protection, and cryptographic key management. These capabilities are central to managing sensitive data securely, reflecting the exam's focus on advanced data protection strategies.</li></ul>
トピック 4	<ul style="list-style-type: none"><li>Management and Security Governance: This topic teaches AWS Security specialists to develop centralized strategies for AWS account management and secure resource deployment. It includes evaluating compliance and identifying security gaps through architectural reviews and cost analysis, essential for implementing governance aligned with certification standards.</li></ul>
トピック 5	<ul style="list-style-type: none"><li>Infrastructure Security: Aspiring AWS Security specialists are trained to implement and troubleshoot security controls for edge services, networks, and compute workloads under this topic. Emphasis is placed on ensuring resilience and mitigating risks across AWS infrastructure. This section aligns closely with the exam's focus on safeguarding critical AWS services and environments.</li></ul>

>> SCS-C02入門知識 <<

## 効率的なSCS-C02入門知識 & 資格試験におけるリーダーオファー & 人気のあるSCS-C02試験資料

SCS-C02学習教材があれば、あなたは自分の夢を叶えます。SCS-C02学習教材はすごく人気があります。全世

界のお客様からいい評価をもらいました。なんといっても、自分はSCS-C02学習教材を利用したら、その資料のよさを感じることができます。大切なのは、SCS-C02学習教材の合格率が高いので、多くのお客様はSCS-C02認定試験資格証明書を取得したということです。

## Amazon AWS Certified Security - Specialty 認定 SCS-C02 試験問題 (Q373-Q378):

### 質問 # 373

A company is migrating one of its legacy systems from an on-premises data center to AWS. The application server will run on AWS, but the database must remain in the on-premises data center for compliance reasons. The database is sensitive to network latency. Additionally, the data that travels between the on-premises data center and AWS must have IPsec encryption. Which combination of AWS solutions will meet these requirements? (Choose two.)

- A. AWS Direct Connect
- B. AWS Site-to-Site VPN
- C. VPC peering
- D. AWS VPN CloudHub
- E. NAT gateway

正解: A、B

解説:

The correct combination of AWS solutions that will meet these requirements is A. AWS Site-to-Site VPN and B. AWS Direct Connect.

A) AWS Site-to-Site VPN is a service that allows you to securely connect your on-premises data center to your AWS VPC over the internet using IPsec encryption. This solution meets the requirement of encrypting the data in transit between the on-premises data center and AWS.

B) AWS Direct Connect is a service that allows you to establish a dedicated network connection between your on-premises data center and your AWS VPC. This solution meets the requirement of reducing network latency between the on-premises data center and AWS.

C) AWS VPN CloudHub is a service that allows you to connect multiple VPN connections from different locations to the same virtual private gateway in your AWS VPC. This solution is not relevant for this scenario, as there is only one on-premises data center involved.

D) VPC peering is a service that allows you to connect two or more VPCs in the same or different regions using private IP addresses. This solution does not meet the requirement of connecting an on-premises data center to AWS, as it only works for VPCs.

E) NAT gateway is a service that allows you to enable internet access for instances in a private subnet in your AWS VPC. This solution does not meet the requirement of connecting an on-premises data center to AWS, as it only works for outbound traffic from your VPC.

### 質問 # 374

Your CTO thinks your IAM account was hacked. What is the only way to know for certain if there was unauthorized access and what they did, assuming your hackers are very sophisticated IAM engineers and doing everything they can to cover their tracks? Please select:

- A. Use IAM Config Timeline forensics.
- B. Use IAM Config SNS Subscriptions and process events in real time.
- C. Use CloudTrail backed up to IAM S3 and Glacier.
- D. Use CloudTrail Log File Integrity Validation.

正解: D

解説:

The IAM Documentation mentions the following

To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it you can use CloudTrail log file integrity validation. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. You can use the IAM CLI to validate the files in the location where CloudTrail delivered them Validated log files are invaluable in security and forensic investigations. For example, a validated log file enables you to assert positively that the log file itself has not changed, or that particular user credentials performed specific API activity. The CloudTrail log file integrity validation process also lets you know if a

log file has been deleted or changed, or assert positively that no log files were delivered to your account during a given period of time.

Options B.C and D is invalid because you need to check for log File Integrity Validation for cloudtrail logs For more information on Cloudtrail log file validation, please visit the below URL:

<http://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html> The correct answer is: Use CloudTrail Log File Integrity Validation.

omit your Feedback/Queries to our Expert

#### 質問 # 375

A company's application team needs to host a MySQL database on IAM. According to the company's security policy, all data that is stored on IAM must be encrypted at rest. In addition, all cryptographic material must be compliant with FIPS 140-2 Level 3 validation.

The application team needs a solution that satisfies the company's security requirements and minimizes operational overhead. Which solution will meet these requirements?

- A. Host the database on an Amazon EC2 instance. Use Transparent Data Encryption (TDE) for encryption and key management.
- B. Host the database on Amazon RDS. Use Amazon Elastic Block Store (Amazon EBS) for encryption. Use an IAM Key Management Service (IAM KMS) custom key store that is backed by IAM CloudHSM for key management.
- C. Host the database on an Amazon EC2 instance. Use Amazon Elastic Block Store (Amazon EBS) for encryption. Use a customer managed CMK in IAM Key Management Service (IAM KMS) for key management.
- **D. Host the database on Amazon RDS. Use Amazon Elastic Block Store (Amazon EBS) for encryption. Use an IAM managed CMK in IAM Key Management Service (IAM KMS) for key management.**

正解: D

#### 質問 # 376

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?

`{resolve:s3:MyBucketName:MyObjectName}}`.

- 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 Amazon DynamoDB. In the template, replace all references to the value with `{{resolve:dynamodb:MyTableName:MyPrimaryKey}}`.
- **C. Store the API key value in AWS Secrets Manager. In the template, replace all references to the value with `{`**
- **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: C

解説:

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 lifecycle<sup>1</sup>. Secrets Manager integrates with AWS CloudFormation, which allows you to reference secrets from your templates using the `{{resolve:secretsmanager:...}}` syntax<sup>2</sup>. 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 Store<sup>3</sup>. 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 tables<sup>4</sup>. 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 buckets<sup>5</sup>. 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.

References:

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 # 377

A company is designing a multi-account structure for its development teams. The company is using AWS Organizations and AWS IAM Identity Center (AWS Single Sign-On). The company must implement a solution so that the development teams can use only specific AWS Regions and so that each AWS account allows access to only specific AWS services. Which solution will meet these requirements with the LEAST operational overhead?

- A. Deactivate AWS Security Token Service (AWS STS) in Regions that the developers are not allowed to use.
- **B. Create SCPs that include the Condition, Resource, and NotAction elements to allow access to only the Regions and services that are needed.**
- C. For each AWS account, create tailored identity-based policies for IAM Identity Center. Use statements that include the Condition, Resource, and NotAction elements to allow access to only the Regions and services that are needed.
- D. Use IAM Identity Center to set up service-linked roles with IAM policy statements that include the Condition, Resource, and NotAction elements to allow access to only the Regions and services that are needed.

正解: B

解説:

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps\\_examples\\_general.html#example-scp-deny-region](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_general.html#example-scp-deny-region)

### 質問 # 378

.....

激変なネット情報時代で、質の良いAmazonのSCS-C02問題集を見つけるために、あなたは悩むことがありますか。私たちは君がGoShikenを選ぶことと正確性の高いAmazonのSCS-C02問題集を祝っています。GoShikenのAmazonのSCS-C02問題集が君の認定試験に合格するのに大変役に立ちます。

SCS-C02試験資料: <https://www.goshiken.com/Amazon/SCS-C02-mondaishu.html>

- Amazon SCS-C02入門知識: 無料ダウンロードAWS Certified Security - Specialty □ 【 [www.goshiken.com](http://www.goshiken.com) 】 から簡単に▶ SCS-C02 □を無料でダウンロードできますSCS-C02関連資料
- SCS-C02復習過去問 □ SCS-C02試験解説問題 □ SCS-C02資料勉強 □ 《 [www.goshiken.com](http://www.goshiken.com) 》を入力して▶ SCS-C02 □を検索し、無料でダウンロードしてくださいSCS-C02受験資格
- 認定するSCS-C02入門知識試験-試験の準備方法-ハイパスレーターのSCS-C02試験資料 □ ➡ [www.passtest.jp](http://www.passtest.jp) □□□から簡単に[ SCS-C02 ]を無料でダウンロードできますSCS-C02資料勉強
- 試験の準備方法-効果的なSCS-C02入門知識試験-実地的なSCS-C02試験資料 □ □ [www.goshiken.com](http://www.goshiken.com) □の無料ダウンロード▶ SCS-C02 □ページが開きますSCS-C02練習問題
- 有効的なSCS-C02入門知識 - 合格スムーズSCS-C02試験資料 |権威のあるSCS-C02参考書 □ ➡ [www.xhs1991.com](http://www.xhs1991.com) □で使える無料オンライン版[ SCS-C02 ] の試験問題SCS-C02資料勉強
- SCS-C02全真模擬試験 □ SCS-C02日本語練習問題 □ SCS-C02模擬モード □ ウェブサイト▶ [www.goshiken.com](http://www.goshiken.com) □から{ SCS-C02 }を開いて検索し、無料でダウンロードしてくださいSCS-C02資料勉強
- Amazon SCS-C02入門知識: 無料ダウンロードAWS Certified Security - Specialty □ ➡ [www.mogicexam.com](http://www.mogicexam.com) □で使える無料オンライン版{ SCS-C02 } の試験問題SCS-C02参考資料
- 素晴らしいSCS-C02入門知識一合格-信頼的なSCS-C02試験資料 □ 《 [www.goshiken.com](http://www.goshiken.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最新版
- Amazon SCS-C02入門知識: 無料ダウンロードAWS Certified Security - Specialty □ □ [www.xhs1991.com](http://www.xhs1991.com) □サイトにて最新▶ SCS-C02 ◁問題集をダウンロードSCS-C02参考資料

- P.S. GoShiken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=1dUPhmeU04Mqdv4sQpAh-m8cjbI8wbffip>