

Amazon SCS-C02熱門題庫和KaoGuTi -保證認證成功，簡便的培訓方式



從Google Drive中免費下載最新的KaoGuTi SCS-C02 PDF版考試題庫：https://drive.google.com/open?id=1uifal_rhAprulrpriK3-Kx5kaTKE2LWm

還在為不知道怎麼通過的SCS-C02認證考試而煩惱嗎？現在終於不用擔心這個問題啦。KaoGuTi多年致力於SCS-C02認證考試的研究，有著豐富的經驗，強大的考古題，幫助你高效率的通過考試。能否成功通過一項考試，並不在於你看了多少東西，而在於你是否找對了方法，KaoGuTi就是你通過SCS-C02認證考試的正確方法！

Amazon SCS-C02 Exam Overview:

Certification Vendor:	Amazon Web Services (AWS)
Exam Name:	AWS Certified Security - Specialty
Exam Number:	SCS-C02
Exam Duration:	190 minutes
Real Exam Qty:	65
Exam Format:	Multiple Choice, Multiple Response

Certificate Validity Period:	3 years
Passing Score:	720 (on a scale of 100-1000)
Available Languages:	English, Japanese, Korean, Simplified Chinese
Exam Price:	\$300 USD
Related Certifications:	AWS Certified Cloud Practitioner AWS Certified Solutions Architect - Associate
Sample Questions:	Amazon SCS-C02 Sample Questions
Exam Way:	Online proctored (PSI) or in-person at testing centers (Pearson VUE)
Pre Condition:	Recommended: AWS Certified Cloud Practitioner or Associate-level certification, plus 2+ years of hands-on security experience
Official Syllabus URL:	https://aws.amazon.com/certification/certified-security-specialty/

>> SCS-C02熱門題庫 <<

確保通過的SCS-C02熱門題庫 |高通過率的考試材料|有用的SCS-C02考試大綱

在這個人才濟濟的社會，人們不斷提高自己的知識想達到更高的水準，但是國家對尖端的IT人員需求量還在不斷擴大，國際上更是如此。所以很多人想通過Amazon的SCS-C02考試認證，但想通過並非易事。其實只要你們選擇一個好的培訓資料完全通過也不是不可能，我們KaoGuTi Amazon的SCS-C02考試認證培訓資料完全擁有這個能力幫助你們通過認證，KaoGuTi網站的培訓資料是通過許多使用過的考生實踐證明了的，而且在國際上一直遙遙領先，如果你要通過Amazon的SCS-C02考試認證，就將KaoGuTi Amazon的SCS-C02考試認證培訓資料加入購物車吧！

Amazon SCS-C02 考試大綱：

主題	簡介
主題 1	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.
主題 2	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.
主題 3	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.
主題 4	Threat Detection and Incident Response: In this topic, AWS Security specialists gain expertise in crafting incident response plans and detecting security threats and anomalies using AWS services. It delves into effective strategies for responding to compromised resources and workloads, ensuring readiness to manage security incidents. Mastering these concepts is critical for handling scenarios assessed in the SCS-C02 exam.
主題 5	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.

最新的 AWS Certified Specialty SCS-C02 免費考試真題 (Q274-Q279):

問題 #274

A company is using IAM Organizations. The company wants to restrict IAM usage to the eu-west-1 Region for all accounts under an OU that is named "development." The solution must persist restrictions to existing and new IAM accounts under the development OU.

- A. Include the following SCP on the development OU:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonDefaultRegions",
      "Effect": "Deny",
      "NotAction": [
        <Desired Global Services> ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": [
            "eu-west-1"
          ]
        }
      },
      "ArnNotLike": {
        "aws:PrincipalARN": "arn:aws:iam::*:role/AWSEExecution"
      }
    }
  ]
}
```

- B. Include the following SCP on the development account:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonDefaultRegions",
      "Effect": "Deny",
      "NotAction": [
        <Desired Global Services> ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": [
            "eu-west-1"
          ]
        }
      },
      "ArnNotLike": {
        "aws:PrincipalARN": "arn:aws:iam::*:role/AWSEExecution"
      }
    }
  ]
}
```

- C. Include the following SCP on the development OU:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonDefaultRegions",
      "Effect": "Deny",
      "NotAction": [
        <Desired Global Services> ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": [
            "eu-west-1"
          ]
        },
        "ArnNotLike": {
          "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
        }
      }
    }
  ]
}
```

- D. Include the following SCP on the development OU:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonDefaultRegions",
      "Effect": "Allow",
      "NotAction": [
        <Desired Global Services> ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": [
            "us-east-1"
          ]
        },
        "ArnNotLike": {
          "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
        }
      }
    }
  ]
}
```

- A. Option C
- **B. Option A**
- C. Option B
- D. Option D

答案: B

問題 #275

A company needs to implement DNS Security Extensions (DNSSEC) for a specific subdomain. The subdomain is already registered with Amazon Route 53. A security engineer has enabled DNSSEC signing and has created a key-signing key (KSK). When the security engineer tries to test the configuration, the security engineer receives an error for a broken trust chain. What should the security engineer do to resolve this error?

- A. Replace the KSK with a zone-signing key (ZSK).
- B. Create a Delegation Signer (DS) record in the subdomain.
- C. Deactivate and then activate the KSK.
- **D. Create a Delegation Signer (DS) record in the parent hosted zone.**

答案: D

問題 #276

A company is using AWS Organizations to implement a multi-account strategy. The company does not have on-premises infrastructure. All workloads run on AWS. The company currently has eight member accounts. The company anticipates that it will have no more than 20 AWS accounts total at any time.

The company issues a new security policy that contains the following requirements:

- * No AWS account should use a VPC within the AWS account for workloads.
- * The company should use a centrally managed VPC that all AWS accounts can access to launch workloads in subnets.
- * No AWS account should be able to modify another AWS account's application resources within the centrally managed VPC.
- * The centrally managed VPC should reside in an existing AWS account that is named Account-A within an organization.

The company uses an AWS CloudFormation template to create a VPC that contains multiple subnets in Account A. This template exports the subnet IDs through the CloudFormation Outputs section.

Which solution will complete the security setup to meet these requirements?

- A. Use a CloudFormation template in the member accounts to launch workloads. Configure the template to use the Fn::ImportValue function to obtain the subnet ID values.
- B. Use a transit gateway in the VPC within Account-A. Configure the member accounts to use the transit gateway to access the subnets in Account-A to launch workloads.
- **C. Use AWS Resource Access Manager (AWS RAM) to share Account-A's VPC subnets with the remaining member accounts. Configure the member accounts to use the shared subnets to launch workloads.**
- D. Create a peering connection between Account-A and the remaining member accounts. Configure the member accounts to use the subnets in Account-A through the VPC peering connection to launch workloads.

答案: C

解題說明:

The correct answer is C. Use AWS Resource Access Manager (AWS RAM) to share Account-A's VPC subnets with the remaining member accounts. Configure the member accounts to use the shared subnets to launch workloads.

This answer is correct because AWS RAM is a service that helps you securely share your AWS resources across AWS accounts, within your organization or organizational units (OUs), and with IAM roles and users for supported resource types¹. One of the supported resource types is VPC subnets², which means you can share the subnets in Account-A's VPC with the other member accounts using AWS RAM. This way, you can meet the requirements of using a centrally managed VPC, avoiding duplicate VPCs in each account, and launching workloads in shared subnets. You can also control the access to the shared subnets by using IAM policies and resource-based policies³, which can prevent one account from modifying another account's resources.

The other options are incorrect because:

A. Using a CloudFormation template in the member accounts to launch workloads and using the Fn::ImportValue function to obtain the subnet ID values is not a solution, because Fn::ImportValue can only import values that have been exported by another stack within the same region⁴. This means that you cannot use Fn::ImportValue to reference the subnet IDs that are exported by Account-A's CloudFormation template, unless all the member accounts are in the same region as Account-A. This option also does not avoid creating duplicate VPCs in each account, which is one of the requirements.

B. Using a transit gateway in the VPC within Account-A and configuring the member accounts to use the transit gateway to access the subnets in Account-A to launch workloads is not a solution, because a transit gateway does not allow you to launch workloads in another account's subnets. A transit gateway is a network transit hub that enables you to route traffic between your VPCs and on-premises networks⁵, but it does not enable you to share subnets across accounts.

D. Creating a peering connection between Account-A and the remaining member accounts and configuring the member accounts to use the subnets in Account-A through the VPC peering connection to launch workloads is not a solution, because a VPC peering

connection does not allow you to launch workloads in another account's subnets. A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately, but it does not enable you to share subnets across accounts.

References:

1: What is AWS Resource Access Manager? 2: Shareable AWS resources 3: Managing permissions for shared resources 4: Fn::ImportValue 5: What is a transit gateway? 6: What is VPC peering?

問題 #277

A company is using IAM Organizations. The company wants to restrict IAM usage to the eu-west-1 Region for all accounts under an OU that is named "development." The solution must persist restrictions to existing and new IAM accounts under the development OU.

- A. Include the following SCP on the development OU:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonDefaultRegions",
      "Effect": "Deny",
      "NotAction": [
        <Desired Global Services> ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": [
            "eu-west-1"
          ]
        }
      },
      "ArnNotLike": {
        "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
      }
    }
  ]
}
```


- B. Include the following SCP on the development account:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonDefaultRegions",
      "Effect": "Deny",
      "NotAction": [
        <Desired Global Services> ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": [
            "eu-west-1"
          ]
        },
        "ArnNotLike": {
          "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
        }
      }
    }
  ]
}
```

- C. Include the following SCP on the development OU:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonDefaultRegions",
      "Effect": "Deny",
      "NotAction": [
        <Desired Global Services> ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": [
            "eu-west-1"
          ]
        },
        "ArnNotLike": {
          "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
        }
      }
    }
  ]
}
```

- D. Include the following SCP on the development OU:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonDefaultRegions",
      "Effect": "Allow",
      "NotAction": [
        "<Desired Global Services>",
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": [
            "us-east-1"
          ]
        },
        "ArnNotLike": {
          "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
        }
      }
    }
  ]
}
```

- A. Option C
- **B. Option A**
- C. Option B
- D. Option D

答案: B

問題 #278

A company is using IAM Secrets Manager to store secrets for its production Amazon RDS database. The Security Officer has asked that secrets be rotated every 3 months. Which solution would allow the company to securely rotate the secrets? (Select TWO.)

- **A. Place the RDS instance in a private subnet and an IAM Lambda function inside the VPC in the private subnet. Configure a Secrets Manager interface endpoint. Schedule the Lambda function to run every 3 months to rotate the secrets.**
- B. Place the RDS instance in a public subnet and an IAM Lambda function outside the VPC. Schedule the Lambda function to run every 3 months to rotate the secrets.
- C. Place the RDS instance in a private subnet and an IAM Lambda function outside the VPC. Configure the private subnet to use an internet gateway. Schedule the Lambda function to run every 3 months to rotate the secrets.
- D. Place the RDS instance in a private subnet and an IAM Lambda function inside the VPC in the private subnet. Schedule the Lambda function to run quarterly to rotate the secrets.
- **E. Place the RDS instance in a private subnet and an IAM Lambda function inside the VPC in the private subnet. Configure the private subnet to use a NAT gateway. Schedule the Lambda function to run every 3 months to rotate the secrets.**

答案: A,E

解題說明:

these are the solutions that can securely rotate the secrets for the production RDS database using Secrets Manager. Secrets Manager is a service that helps you manage secrets such as database credentials, API keys, and passwords. You can use Secrets Manager to rotate secrets automatically by using a Lambda function that runs on a schedule. The Lambda function needs to have access to both the RDS instance and the Secrets Manager service. Option B places the RDS instance in a private subnet and the Lambda function in the same VPC in another private subnet. The private subnet with the Lambda function needs to use a NAT gateway to access Secrets Manager over the internet. Option E places the RDS instance and the Lambda function in the same private subnet and configures a Secrets Manager interface endpoint, which is a private connection between the VPC and Secrets Manager. The other options are either insecure or incorrect for rotating secrets using Secrets Manager.

.....

GGG G02 译词书式 ● GGG G02 资源 □ GGG G02 题库更新资源

- P.S. KaoGuTi在Google Drive上分享了免費的、最新的SCS-C02考試題庫：https://drive.google.com/open?id=1u1al_rhApru1rprIK3-Kx5kaTKE2LWm

P.S. KaoGuTi在Google Drive上分享了免費的、最新的SCS-C02考試題庫：https://drive.google.com/open?id=1ui1al_rhApru1rprIK3-Kx5kaTKE2LWm