SCS-C02 Dumps Deutsch, SCS-C02 Originale Fragen

P.S. Kostenlose 2026 Amazon SCS-C02 Prüfungsfragen sind auf Google Drive freigegeben von DeutschPrüfung verfügbar: https://drive.google.com/open?id=1ZrtR5yu9qY6NJ5IN9iO4idCRN4guClTn

Warum wählen viele Leute die Schulungsunterlagen zur Amazon SCS-C02 Zertifizierungsprüfung von DeutschPrüfung? Es gibt auch andere Websites, die Schulungsressourcen zur SCS-C02 Zertifizierungsprüfung bietet. Unser DeutschPrüfung stellt Ihnen die echten Prüfungsmaterialien zur Verfügung. Unser Eliteteam, Zertifizierungsexperten, Techniker und berühmte Linguisten bearbeiten die neueste Amazon SCS-C02 Zertifizierungsprüfung. Deshalb klicken Sie DeutschPrüfung Website, wenn Sie die Amazon SCS-C02 Zertifizierungsprüfung bestehen wollen. Mit DeutschPrüfung können Sie Ihren Traum Schritt für Schritt verwirklichen.

Amazon SCS-C02 Prüfungsplan:

Thema	Einzelheiten
Thema 1	• 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.
Thema 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.

Thema 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.

>> SCS-C02 Dumps Deutsch <<

Amazon SCS-C02 Originale Fragen - SCS-C02 Prüfungsinformationen

Viele Leute, die in der IT-Branche arbeiten, wissen die mühsame Vorbereitung auf die Amazon SCS-C02 Prüfung. Wir DeutschPrüfung können doch den Schwierigkeitsgrad der Amazon SCS-C02 Prüfung nicht ändern, aber wir können die Schwierigkeitsgrad der Vorbereitung für Sie vermindern. Ihre Angst vor der Amazon SCS-C02 Prüfung wird beseitigen, solange Sie die Prüfungsunterlagen von unserem Technik-Team probiert haben. Wir tun unser Bestes, um Ihnen zu helfen, Ihre Konfidenz für Amazon SCS-C02 zu verstärken!

Amazon AWS Certified Security - Specialty SCS-C02 Prüfungsfragen mit Lösungen (Q447-Q452):

447. Frage
A security engineer needs to create an IAM Key Management Service <IAM KMS) key that will De used to encrypt all data stored in a company's Amazon S3 Buckets in the us-west-1 Region. The key will use server-side encryption. Usage of the key must be limited to requests coming from Amazon S3 within the company's account.
Which statement in the KMS key policy will meet these requirements?

- A.

```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": "s3.us-west-1.amazonaws.com",
            "kms:CallerAccount": "<CustomerAccountID>"
        }
    }
}
```

```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "s3.us-west-1.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:CallerAccount": "<CustomerAccountID>"
        }
    }
}
```

- B.

```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:aws:s3:arn": [
                "arn:aws:s3:::*"
            ],
```

- C.

Antwort: A

448. Frage
A Systems Engineer is troubleshooting the connectivity of a test environment that includes a virtual security appliance deployed inline. In addition to using the virtual security appliance, the Development team wants to use security groups and network ACLs to accomplish various security requirements in the environment.
What configuration is necessary to allow the virtual security appliance to route the traffic?

- A. Disable network ACLs.
- B. Disable the Network Source/Destination check on the security appliance's elastic network interface
- C. Configure the security appliance's elastic network interface for promiscuous mode.
- D. Place the security appliance in the public subnet with the internet gateway

Antwort: B

Begründung:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#eni-basics Source/destination checking "You must disable source/destination checks if the instance runs services such as network address translation, routing, or firewalls." The correct answer is C) Disable the Network Source/Destination check on the security appliance's elastic network interface.
This answer is correct because disabling the Network Source/Destination check allows the virtual security appliance to route traffic

that is not addressed to or from itself. By default, this check is enabled on all EC2 instances, and it prevents them from forwarding traffic that does not match their own IP or MAC addresses. However, for a virtual security appliance that acts as a router or a firewall, this check needs to be disabled, otherwise it will drop the traffic that it is supposed to route12.
The other options are incorrect because:
A) Disabling network ACLs is not a solution, because network ACLs are optional layers of security for the subnets in a VPC. They can be used to allow or deny traffic based on IP addresses and ports, but they do not affect the routing behavior of the virtual security appliance3.
B) Configuring the security appliance's elastic network interface for promiscuous mode is not a solution, because promiscuous mode is a mode for a network interface that causes it to pass all traffic it receives to the CPU, rather than passing only the frames that it is programmed to receive. Promiscuous mode is normally used for packet sniffing or monitoring, but it does not enable the network interface to route traffic4.
D) Placing the security appliance in the public subnet with the internet gateway is not a solution, because it does not address the routing issue of the virtual security appliance. The security appliance can be placed in either a public or a private subnet, depending on the network design and security requirements, but it still needs to have the Network Source/Destination check disabled to route traffic properly5.
Reference:
1: Enabling or disabling source/destination checks - Amazon Elastic Compute Cloud 2: Virtual security appliance - Wikipedia 3: Network ACLs - Amazon Virtual Private Cloud 4: Promiscuous mode - Wikipedia 5: NAT instances - Amazon Virtual Private Cloud

449. Frage
A company has an AWS Key Management Service (AWS KMS) customer managed key with imported key material Company policy requires all encryption keys to be rotated every year What should a security engineer do to meet this requirement for this customer managed key?

- A. Create a new customer managed key Import new key material to the new key Point the key alias to the new key
- B. Enable automatic key rotation annually for the existing customer managed key
- C. Use the AWS CLI to create an AWS Lambda function to rotate the existing customer managed key annually
- D. Import new key material to the existing customer managed key Manually rotate the key

Antwort: B

Begründung:
Explanation
To meet the requirement of rotating the AWS KMS customer managed key every year, the most appropriate solution would be to enable automatic key rotation annually for the existing customer managed key. This will ensure that AWS KMS generates new cryptographic material for the CMK every year. AWS KMS also saves the CMK's older cryptographic material in perpetuity so it can be used to decrypt data that it encrypted. AWS KMS does not delete any rotated key material until you delete the CMK.
References: : Key Rotation Enabled | Trend Micro : Rotating AWS KMS keys - AWS Key Management Service

450. Frage
A company has configured an organization in AWS Organizations for its AWS accounts. AWS CloudTrail is enabled in all AWS Regions. A security engineer must implement a solution to prevent CloudTrail from being disabled. Which solution will meet this requirement?

- A. Create 1AM policies for all the company's users to prevent the users from performing the DescribeTrails action and the GetTrailStatus action.
- B. Enable server-side encryption with AWS KMS keys (SSE-KMS) for CloudTrail logs. Create a KMS key Attach a policy to the key to prevent decryption of the logs
- C. Enable CloudTrail log file integrity validation from the organization's management account.
- D. Create an SCP that includes an explicit Deny rule for the StopLogging action and the DeleteTrail action. Attach the SCP to the root OU.

Antwort: D

Begründung:
Understand the Risk:
Unauthorized users could stop or delete CloudTrail logging, creating a gap in audit trails.
Create a Service Control Policy (SCP):

Define an SCP at the root organizational unit (OU) level. The SCP should explicitly denyStopLoggingandDeleteTrailactions.
Example SCP:
{
"Version": "2012-10-17",
"Statement":
[
{
"Effect": "Deny",
"Action":
[
"cloudtrail:StopLogging",
"cloudtrail:DeleteTrail"
],
"Resource": "*"
}
]
}
Attach the SCP:
Attach the SCP to the root OU in AWS Organizations. This ensures the policy is enforced across all accounts within the organization.
Test and Verify:
Attempt to stop or delete a CloudTrail trail to ensure the SCP prevents these actions.
AWS CloudTrail Security Best Practices
Service Control Policies Documentation

451. Frage
An AWS Lambda function was misused to alter data, and a security engineer must identify who invoked the function and what output was produced. The engineer cannot find any logs create