SCS-C02考試 & SCS-C02更新

從Google Drive中免費下載最新的Testpdf SCS-C02 PDF版考試題庫：https://drive.google.com/open?id=1fYJsHkJB2sDCqeW2MxWw4rIzPPABR-dC

在如今競爭激烈的IT行業中，通過了Amazon SCS-C02 認證考試是有很多好處的。因為有了Amazon SCS-C02 認證證書就可以提高收入。拿到了Amazon SCS-C02 認證證書的人往往要比沒有證書的同行工資高很多。可是Amazon SCS-C02 認證考試不是很容易通過的，所以Testpdf是一個可以幫助你增長收入的網站.

Amazon SCS-C02 考試大綱：

主題	簡介
主題 1	• 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.
主題 2	• 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 3	• 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 4	• 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考試 <<

Amazon SCS-C02更新 - 新版SCS-C02考古題

Amazon的SCS-C02認證考試是現在IT領域非常有人氣的考試。取得這個考試的認證資格對想晉升的人們來說是最好的，也是最可以看到效果的選擇。而且，借助這個考試你也可以提高自己的技能，掌握更多的對工作有用的技術。這樣你就可以更好地完成你的工作，向別人展示你的超強的能力。也只有这样你才可以获得更多的发展机会。

最新的 AWS Certified Specialty SCS-C02 免費考試真題 (Q57-Q62):

問題 #57
A corporation is preparing to acquire several companies. A Security Engineer must design a solution to ensure that newly acquired IAM accounts follow the corporation's security best practices. The solution should monitor each Amazon S3 bucket for unrestricted public write access and use IAM managed services.
What should the Security Engineer do to meet these requirements?

- A. Set up IAM Systems Manager to monitor S3 bucket policies for public write access.
- B. Configure Amazon Macie to continuously check the configuration of all S3 buckets.
- C. Configure an Amazon EC2 instance to have an IAM role and a cron job that checks the status of all S3 buckets.
- D. Enable IAM Config to check the configuration of each S3 bucket.

答案：A

解題說明：
Explanation
because this is a solution that can monitor each S3 bucket for unrestricted public write access and use IAM managed services. S3 is a service that provides object storage in the cloud. Systems Manager is a service that helps you automate and manage your AWS resources. You can use Systems Manager to monitor S3 bucket policies for public write access by using a State Manager association that runs a predefined document called AWS-FindS3BucketWithPublicWriteAccess. This document checks each S3 bucket in an account and reports any bucket that has public write access enabled. The other options are either not suitable or not feasible for meeting the requirements.

問題 #58
A Security Engineer is troubleshooting an issue with a company's custom logging application. The application logs are written to an Amazon S3 bucket with event notifications enabled to send events lo an Amazon SNS topic. All logs are encrypted at rest using an IAM KMS CMK. The SNS topic is subscribed to an encrypted Amazon SQS queue. The logging application polls the queue for new messages that contain metadata about the S3 object. The application then reads the content of the object from the S3 bucket for indexing.
The Logging team reported that Amazon CloudWatch metrics for the number of messages sent or received is showing zero. No togs are being received.
What should the Security Engineer do to troubleshoot this issue?
A) Add the following statement to the IAM managed CMKs:
B)
Add the following statement to the CMK key policy:
C)
Add the following statement to the CMK key policy:
D)
Add the following statement to the CMK key policy:

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

答案：D

問題 #59
A security engineer is designing an IAM policy to protect AWS API operations. The policy must enforce multi-factor authentication (MFA) for IAM users to access certain services in the AWS production account.
Each session must remain valid for only 2 hours. The current version of the IAM policy is as follows:
Which combination of conditions must the security engineer add to the IAM policy to meet these requirements? (Select TWO.)

- A. "B001 " : " aws : MultiFactorAuthPresent": "false" }
- B. "Bool " : " aws : Multi FactorAuthPresent": "true" }
- C. "NumericGreaterThan" : { " aws : MultiFactorAuthAge " : "7200"

- D. "NumericLessThan" : { "MaxSessionDuration " : "7200"}
- E. "NumericLessThan" : { " aws : Multi FactorAuthAge" : "7200"}

答案： B,E

解題說明：
The correct combination of conditions to add to the IAM policy is A and C. These conditions will ensure that IAM users must use MFA to access certain services in the AWS production account, and that each session will expire after 2 hours.
* Option A: "Bool" : { "aws:MultiFactorAuthPresent" : "true" } is a valid condition that checks if the principal (the IAM user) has authenticated with MFA before making the request. This condition will enforce MFA for the IAM users to accessthe specified services.This condition key is supported by all AWS services that support IAM policies1.
* Option B: "Bool" : { "aws:MultiFactorAuthPresent" : "false" } is the opposite of option A. This condition will allow access only if the principal has not authenticated with MFA, which is not the desired requirement.This condition key is supported by all AWS services that support IAM policies1.
* Option C: "NumericLessThan" : { "aws:MultiFactorAuthAge" : "7200" } is a valid condition that checks if the time since the principal authenticated with MFA is less than 7200 seconds (2 hours). This condition will enforce the session duration limit for the IAM users.This condition key is supported by all AWS services that support IAM policies1.
* Option D: "NumericGreaterThan" : { "aws:MultiFactorAuthAge" : "7200" } is the opposite of option C: This condition will allow access only if the time since the principal authenticated with MFA is more than 7200 seconds (2 hours), which is not the desired requirement.This condition key is supported by all AWS services that support IAM policies1.
* Option E: "NumericLessThan" : { "MaxSessionDuration" : "7200" } is not a valid condition key.
MaxSessionDuration is a property of an IAM role, not a condition key. It specifies the maximum session duration (in seconds) for the role, which can be between 3600 and 43200 seconds (1 to 12 hours).This property can be set when creating or modifying arole, but it cannot be used as a condition in a policy2.

問題 #60
A company has created a set of AWS Lambda functions to automate incident response steps for incidents that occur on Amazon EC2 instances. The Lambda functions need to collect relevant artifacts, such as instance ID and security group configuration. The Lambda functions must then write a summary to an Amazon S3 bucket.
The company runs its workloads in a VPC that uses public subnets and private subnets. The public subnets use an internet gateway to access the internet. The private subnets use a NAT gateway to access the internet.
All network traffic to Amazon S3 that is related to the incident response process must use the AWS network.
This traffic must not travel across the internet.
Which solution will meet these requirements?

- A. Deploy the Lambda functions to a private subnet in the VPC. Create an S3 gateway endpoint to access the S3 service.
- B. Deploy the Lambda functions to a private subnet in the VPC. Configure the Lambda functions to access the S3 service through the NAT gateway.
- C. Deploy an Amazon Simple Queue Service (Amazon SOS) queue and the Lambda functions in the same private subnet. Configure the Lambda functions to send data to the SQS queue. Configure the SOS queue to send data to the S3 bucket.
- D. Deploy the S3 bucket and the Lambda functions in the same private subnet. Configure the Lambda functions to use the default endpoint for the S3 service.

答案： A

解題說明：
* Understanding the Requirements:
* The Lambda functions need access to S3 for writing summaries.
* All traffic to S3 must stay within the AWS network and not traverse the internet.
* Deploy Lambda Functions in a Private Subnet:
* Place the Lambda functions in a private subnet to ensure they do not directly access the internet.
* Create an S3 Gateway Endpoint:
* Set up a VPC gateway endpoint for Amazon S3.
* The endpoint ensures all traffic to S3 stays within AWS's private network.
* Update Route Table:
* Modify the route table for the private subnet to include the gateway endpoint.
* IAM Permissions for the Lambda Function:
* Ensure the Lambda function's execution role has permissions to write to the specified S3 bucket.
Advantages:
* Cost-Effective: Eliminates NAT gateway costs for S3 traffic.

* Secure: Keeps all S3 traffic within AWS's private network.
VPC Endpoint for Amazon S3
Using Lambda in VPC

問題 #61
A company is running internal microservices on Amazon Elastic Container Service (Amazon ECS) with the Amazon EC2 launch type. The company is using Amazon Elastic Container Registry (Amazon ECR) private repositories.
A security engineer needs to encrypt the private repositories by using AWS Key Management Service (AWS KMS). The security engineer also needs to analyze the container images for any common vulnerabilities and exposures (CVEs).
Which solution will meet these requirements?

- A. Enable KMS encryption on the existing ECR repositories. Install Amazon Inspector Agent from the ECS container instances' user data. Run an assessment with the CVE rules.
- B. Recreate the ECR repositories with KMS encryption and ECR scanning enabled. Install AWS Systems Manager Agent on the ECS container instances. Run an inventory report.
- C. Recreate the ECR repositories with KMS encryption and ECR scanning enabled. Analyze the scan report after the next push of images.
- D. Enable KMS encryption on the existing ECR repositories. Use AWS Trusted Advisor to check the ECS container instances and to verify the findings against a list of current CVEs.

答案：C

解題說明：
https://docs.aws.amazon.com/AmazonECR/latest/userguide/repository-create.html
https://docs.aws.amazon.com/AmazonECR/latest/userguide/repository-edit.html

問題 #62
.....

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

此外，這些Testpdf SCS-C02考試題庫的部分內容現在是免費的：https://drive.google.com/open?id=1fYJsHkJB2sDCqeW2MxWw4rIzPPABR-dC