SCS-C02시험대비최신버전덤프최신버전인증덤프자료

2026 DumpTOP 최신 SCS-C02 PDF 버전 시험 문제집과 SCS-C02 시험 문제 및 답변 무료 공유: https://drive.google.com/open?id=1u8gmCJffNEzTvyJXHjJPUevBJojoo6Gv

DumpTOP는 아주 믿을만하고 서비스 또한 만족스러운 사이트입니다. 만약 SCS-C02시험실패 시 우리는 100% 덤프 비용 전액환불 해드립니다.그리고 시험을 패스하여도 우리는 일 년 동안 무료업뎃을 제공합니다.

Amazon SCS-C02 시험요강:

주제	소개
주제 1	• 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.
주제 2	• 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.
주제 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.
주제 4	• 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.

>> SCS-C02시험대비 최신버전 덤프 <<

시험패스 가능한 SCS-C02시험대비 최신버전 덤프 덤프 샘플문제 다운

현재 경쟁울이 심한IT시대에,Amazon SCS-C02자격증 취득만으로 이 경쟁이 심한 사회에서 자신만의위치를 보장할 수 있고 더욱이는 한층업된 삶을 누릴수 있을수도 있습니다. 우리DumpTOP 에서 여러분은Amazon SCS-C02관련 학습지도서를 얻을 수 있습니다. 우리DumpTOP는 IT업계엘리트 한 강사들이 퍼펙트한Amazon SCS-C02문제집을 만들어서 제공합니다. 우리가 제공하는Amazon SCS-C02문제와 답으로 여러분은 한번에 성공적으로 시험을 패스 하실수 있습니다. 중요한것 저희 문제집을 선택함으로 여러분의 시간도 절약해드리고 무엇보다도 많은 근심없이 심

플하게 시험을 패스하여 좋다는 점입니다.

최신 AWS Certified Specialty SCS-C02 무료샘플문제 (Q311-Q316):

질문 # 311
A company suspects that an attacker has exploited an overly permissive role to export credentials from Amazon EC2 instance metadata. The company uses Amazon GuardDuty and AWS Audit Manager. The company has enabled AWS CloudTrail logging and Amazon CloudWatch logging for all of its AWS accounts.
A security engineer must determine if the credentials were used to access the company's resources from an external account.
Which solution will provide this information?

- A. Review GuardDuty findings to find InstanceCredentialExfiltration events.
- B. Review CloudWatch logs for GetSessionToken API calls to AWS Security Token Service (AWS STS) that come from an account ID from outside the company.
- C. Review CloudTrail logs for GetSessionToken API calls to AWS Security Token Service (AWS STS) that come from an account ID from outside the company.
- D. Review assessment reports in the Audit Manager console to find InstanceCredentialExfiltration events.

정답：A

설명：
GuardDuty can detect and alert on EC2 instance credential exfiltration events. These events indicate that the credentials obtained from the EC2 instance metadata service are being used from an IP address that is owned by a different AWS account than the one that owns the instance. GuardDuty can also provide details such as the source and destination IP addresses, the AWS account ID of the attacker, and the API calls made using the exfiltrated credentials.
https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types- iam.html#unauthorizedaccess-iam-instancecredentialexfiltrationoutsideaws

질문 # 312
A company's security engineer is developing an incident response plan to detect suspicious activity in an AWS account for VPC hosted resources. The security engineer needs to provide visibility for as many AWS Regions as possible.
Which combination of steps will meet these requirements MOST cost-effectively? (Select TWO.)

- A. Turn on VPC Flow Logs for all VPCs in the account.
- B. Activate Amazon Detective across all AWS Regions.
- C. Activate Amazon GuardDuty across all AWS Regions.
- D. Create an AWS Lambda function. Create an Amazon EventBridge rule that in-vokes the Lambda function to publish findings to Amazon Simple Email Ser-vice (Amazon SES).
- E. Create an Amazon Simple Notification Service (Amazon SNS) topic. Create an Amazon EventBridge rule that responds to findings and publishes the find-ings to the SNS topic.

정답：C,E

설명：
To detect suspicious activity in an AWS account for VPC hosted resources, the security engineer needs to use a service that can monitor network traffic and API calls across all AWS Regions. Amazon GuardDuty is a threat detection service that can do this by analyzing VPC Flow Logs, AWS CloudTrail event logs, and DNS logs. By activating GuardDuty across all AWS Regions, the security engineer can provide visibility for as many regions as possible. GuardDuty generates findings that contain details about the potential threats detected in the account. To respond to these findings, the security engineer needs to create a mechanism that can notify the relevant stakeholders or take remedial actions. One way to do this is to use Amazon EventBridge, which is a serverless event bus service that can connect AWS services and third-party applications. By creating an EventBridge rule that responds to GuardDuty findings and publishes them to an Amazon Simple Notification Service (Amazon SNS) topic, the security engineer can enable subscribers of the topic to receive notifications via email, SMS, or other methods. This is a cost-effective solution that does not require any additional infrastructure or code.

질문 # 313
A company is designing a multi-account structure for its development teams. The company is using AWS Organizations and AWS Single Sign-On (AWS SSO). 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. Use AWS SSO 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.
- C. Create SCPs that include the Condition, Resource, and NotAction elements to allow access to only the Regions and services that are needed.
- D. For each AWS account, create tailored identity-based policies for AWS SSO. Use statements that include the Condition, Resource, and NotAction elements to allow access to only the Regions and services that are needed.

정답： C

질문 # 314
A company has an application that uses an Amazon RDS PostgreSQL database. The company is developing an application feature that will store sensitive information for an individual in the database.
During a security review of the environment, the company discovers that the RDS DB instance is not encrypting data at rest. The company needs a solution that will provide encryption at rest for all the existing data and for any new data that is entered for an individual.
Which combination of options can the company use to meet these requirements? (Select TWO.)

- A. Create a snapshot of the DB instance. Enable encryption on the snapshoVUse the snapshot to restore the DB instance.
- B. Use IAM Key Management Service (IAM KMS) to create a new default IAM managed awa/rds key. Select this key as the encryption key for operations with Amazon RDS.
- C. Use IAM Key Management Service (IAM KMS] to create a new CMK. Select this key as the encryption key for operations with Amazon RDS.
- D. Create a snapshot of the DB instance. Copy the snapshot to a new snapshot, and enable encryption for the copy process. Use the new snapshot to restore the DB instance.
- E. Modify the configuration of the DB instance by enabling encryption. Create a snapshot of the DB instance. Use the snapshot to restore the DB instance.

정답： A,B

질문 # 315
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 Amazon DynamoDB. In the template, replace all references to the value with {{resolve:dynamodb:MyTableName:MyPrimaryKey}}.
- B. 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}}.
- C. Store the API key value in a new Amazon S3 bucket. In the template, replace all references to the value with {{resolve:s3:...}}
- D. Store the API key value in AWS Secrets Manager. In the template, replace all references to the value with {{resolve:secretsmanager:MySecretId:SecretString}}.

정답： D

설명：
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 lifecycle1. Secrets Manager integrates with AWS CloudFormation, which allows you to reference secrets from your templates using the

{{resolve:secretsmanager:...}} syntax2. 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 Store3. 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 tables4. 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 buckets5. 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)

질문 # 316
.....

그리고 DumpTOP SCS-C02 시험 문제집의 전체 버전을 클라우드 저장소에서 다운로드할 수 있습니다:
https://drive.google.com/open?id=1u8gmCJffNEzTvyJXHjJPUevBJojoo6Gv