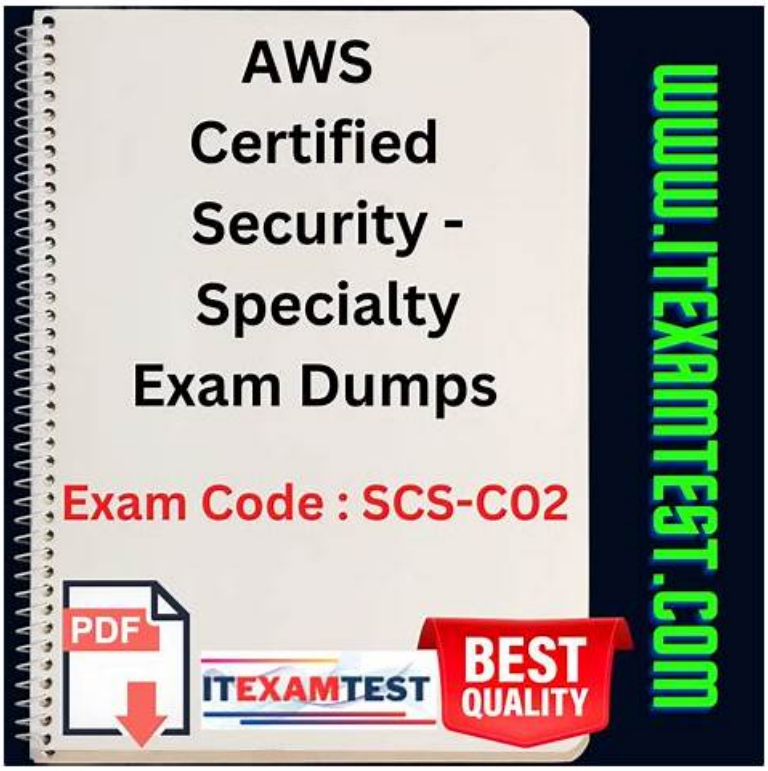
SCS-C02 Dumps Free - Exam SCS-C02 Collection



P.S. Free & New SCS-C02 dumps are available on Google Drive shared by BraindumpsPrep: https://drive.google.com/open?id=1mebL1sErgCuMq88PLhrEEYxeI3EoWOuY

You know, the SCS-C02 certification is tough and difficult IT certification. In order to get a better life, many people as you still want to chase after it. There is a useful and reliable study material of Amazon SCS-C02 actual test for you. The SCS-C02 Pdf Dumps will teach you the basic technology and tell you how to affectively prepare for the SCS-C02 real test. In a word, SCS-C02 updated dumps is the best reference for you preparation.

Amazon SCS-C02 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.
Topic 2	• 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.
Topic 3	• 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.
Topic 4	• 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.

Topic 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.

Exam SCS-C02 Collection, SCS-C02 Materials

To get success in exams and especially in a professional certification test like the AWS Certified Security - Specialty SCS-C02 test is very important to build a bright career. People from all over the world can get the best-paying jobs after passing the Amazon SCS-C02 Exam. So BraindumpsPrep will help you to study well for the AWS Certified Security - Specialty SCS-C02 certification exam. And price is benefit and reliable.

Amazon AWS Certified Security - Specialty Sample Questions (Q335-Q340):

NEW QUESTION # 335
A security engineer is configuring account-based access control (ABAC) to allow only specific principals to put objects into an Amazon S3 bucket. The principals already have access to Amazon S3.
The security engineer needs to configure a bucket policy that allows principals to put objects into the S3 bucket only if the value of the Team tag on the object matches the value of the Team tag that is associated with the principal. During testing, the security engineer notices that a principal can still put objects into the S3 bucket when the tag values do not match.
Which combination of factors are causing the PutObject operation to succeed when the tag values are different? (Choose two.)

- A. The S3 bucket's resource policy does not deny access to put objects.
- B. The S3 bucket's resource policy cannot allow actions to the principal.
- C. The principal's identity-based policy overrides the condition because the identity-based policy contains an explicit allow.
- D. The bucket policy does not apply to principals in the same zone of trust.
- E. The principal's identity-based policy grants access to put objects into the S3 bucket with no conditions.

Answer: A,E

NEW QUESTION # 336
A company is evaluating its security posture. In the past, the company has observed issues with specific hosts and host header combinations that affected the company's business. The company has configured AWS WAF web ACLs as an initial step to mitigate these issues.
The company must create a log analysis solution for the AWS WAF web ACLs to monitor problematic activity. The company wants to process all the AWS WAF logs in a central location. The company must have the ability to filter out requests based on specific hosts.
A security engineer starts to enable access logging for the AWS WAF web ACLs.
What should the security engineer do next to meet these requirements with the MOST operational efficiency?

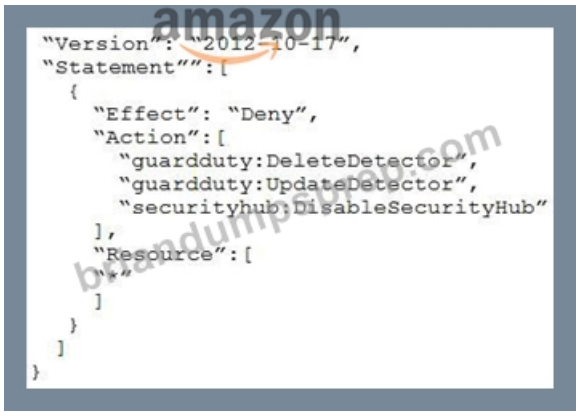
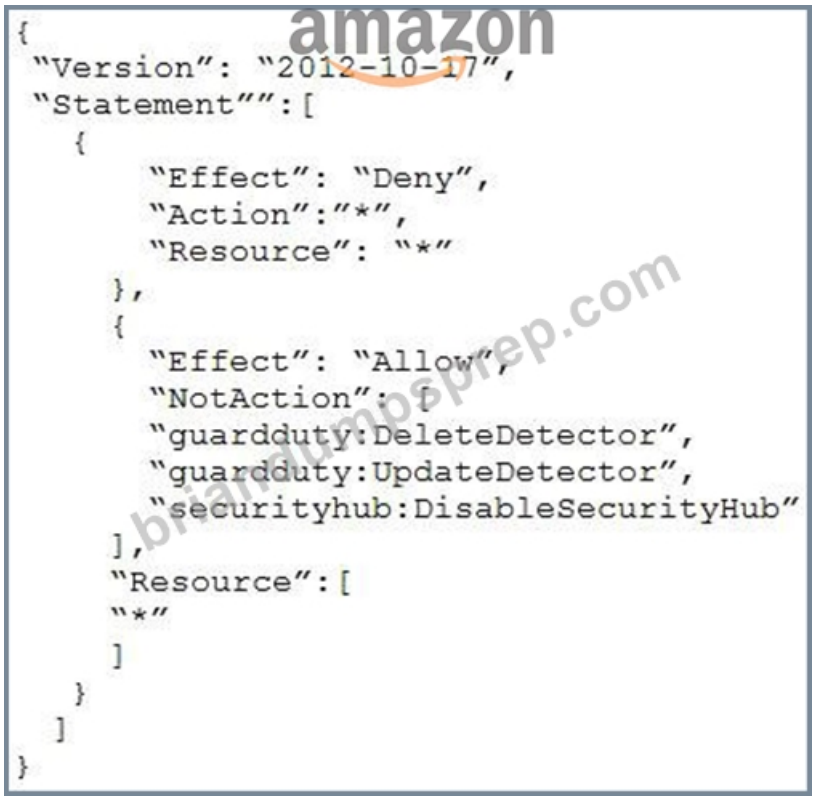
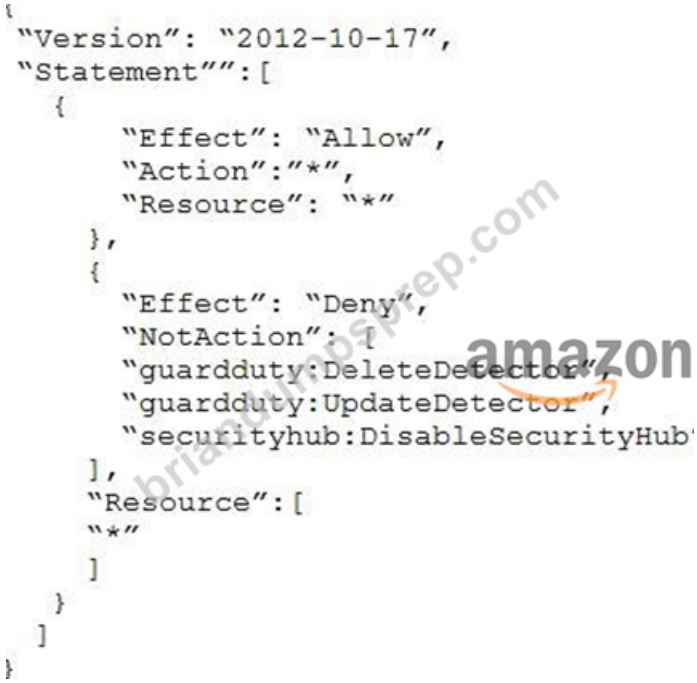
- A. Specify Amazon Redshift as the destination for the access logs. Deploy the Amazon Athena Redshift connector. Use Athena to query the data from Amazon Redshift and to filter the logs by host.
- B. Specify Amazon CloudWatch as the destination for the access logs. Use Amazon CloudWatch Logs Insights to design a query to filter the logs by host.
- C. Specify Amazon CloudWatch as the destination for the access logs. Use Amazon Redshift Spectrum to query the logs and to filter the logs by host.
- D. Specify Amazon CloudWatch as the destination for the access logs. Export the CloudWatch logs to an Amazon S3 bucket. Use Amazon Athena to query the logs and to filter the logs by host.

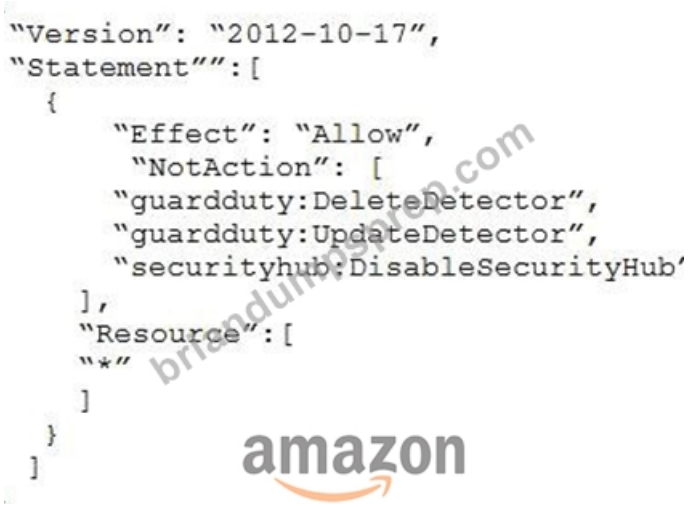
Answer: D

Explanation:
The correct answer is C. Specify Amazon CloudWatch as the destination for the access logs. Export the CloudWatch logs to an Amazon S3 bucket. Use Amazon Athena to query the logs and to filter the logs by host.

According to the AWS documentation1, AWS WAF offers logging for the traffic that your web ACLs analyze. The logs include information such as the time that AWS WAF received the request from your protected AWS resource, detailed information about the request, and the action setting for the rule that the request matched. You can send yourlogs to an Amazon CloudWatch Logs log group, an Amazon Simple Storage Service (Amazon S3) bucket, or an Amazon Kinesis Data Firehose.
To create a log analysis solution for the AWS WAF web ACLs, you can use Amazon Athena, which is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL2. You can use Athena to query and filter the AWS WAF logs by host or any other criteria. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run.
To use Athena with AWS WAF logs, you need to export the CloudWatch logs to an S3 bucket.You can do this by creating a subscription filter that sends your log events to a Kinesis Data Firehose delivery stream, which then delivers the data to an S3 bucket3.Alternatively, you can use AWS DMS to migrate your CloudWatch logs to S34.
After you have exported your CloudWatch logs to S3, you can create a table in Athena that points to your S3 bucket and use the AWS service log format that matches your log schema5. For example, if you are using format for your AWS WAF logs, you can use the AWSSerDe serde. Then you can run SQL queries on your Athena table and filter the results by host or any other field in your log data.
Therefore, this solution meets the requirements of creating a log analysis solution for the AWS WAF web ACLs with the most operational efficiency. This solution does not require setting up any additional infrastructure or services, and it leverages the existing capabilities of CloudWatch, S3, and Athena.
The other options are incorrect because:
A: Specifying Amazon Redshift as the destination for the access logs is not possible, because AWS WAF does not support sending logs directly to Redshift. You would need to use an intermediate service such as Kinesis Data Firehose or AWS DMS to load the data from CloudWatch or S3 to Redshift.Deploying the Amazon Athena Redshift connector is not necessary, because you can query Redshift data directly from Athena without using a connector6. This solution would also incur additional costs and operational overhead of managing a Redshift cluster.
B: Specifying Amazon CloudWatch as the destination for the access logs is possible, but using Amazon CloudWatch Logs Insights to design a query to filter the logs by host is not efficient or scalable.CloudWatch Logs Insights is a feature that enables you to interactively search and analyze your log data in CloudWatch Logs7.However, CloudWatch Logs Insights has somelimitations, such as a maximum query duration of 20 minutes, a maximum of 20 log groups per query, and a maximum retention period of 24 months8. These limitations may affect your ability to perform complex and long-running analysis on your AWS WAF logs.
D: Specifying Amazon CloudWatch as the destination for the access logs is possible, but using Amazon Redshift Spectrum to query the logs and filter them by host is not efficient or cost-effective.Redshift Spectrum is a feature of Amazon Redshift that enables you to run queries against exabytes of data in S3 without loading or transforming any data9. However, Redshift Spectrum requires a Redshift cluster to process the queries, which adds additional costs and operational overhead.Redshift Spectrum also charges you based on the number ofbytes scanned by each query, which can be expensive if you have large volumes of log data10.
References:
1:Logging AWS WAF web ACL traffic - AmazonWeb Services2:What Is Amazon Athena? - Amazon Athena3:Streaming CloudWatch Logs Data to Amazon S3 - Amazon CloudWatch Logs4:Migrate data from CloudWatch Logs using AWS Database Migration Service - AWS Database Migration Service5:Querying AWS service logs - Amazon Athena6:Querying data from Amazon Redshift - Amazon Athena7:Analyzing log data with CloudWatch LogsInsights - Amazon CloudWatch Logs8:CloudWatch Logs Insights quotas - Amazon CloudWatch9:Querying external data using Amazon Redshift Spectrum - Amazon Redshift10: Amazon Redshift Spectrum pricing - Amazon Redshift

NEW QUESTION # 337
A company deploys a set of standard IAM roles in AWS accounts. The IAM roles are based on job functions within the company. To balance operational efficiency and security, a security engineer implemented AWS Organizations SCPs to restrict access to critical security services in all company accounts.
All of the company's accounts and OUs within AWS Organizations have a default FullAWSAccess SCP that is attached. The security engineer needs to ensure that no one can disable Amazon GuardDuty and AWS Security Hub. The security engineer also must not override other permissions that are granted by IAM policies that are defined in the accounts.
Which SCP should the security engineer attach to the root of the organization to meet these requirements?

- A.

"Version": "2012-10-17",
"Statement"":[
{
"Effect": "Deny",
"Action":[
"guardduty:DeleteDetector",
"guardduty:UpdateDetector",
"securityhub:DisableSecurityHub"
],
"Resource":[
"*"
]
}
]
}
- B.

{
"Version": "2012-10-17",
"Statement"":[
{
"Effect": "Deny",
"Action":"*",
"Resource": "*"
},
{
"Effect": "Allow",
"NotAction": [
"guardduty:DeleteDetector",
"guardduty:UpdateDetector",
"securityhub:DisableSecurityHub"
],
"Resource":[
"*"
]
}
]
}
- C.

{
"Version": "2012-10-17",
"Statement"":[
{
"Effect": "Allow",
"Action":"*",
"Resource": "*"
},
{
"Effect": "Deny",
"NotAction": [
"guardduty:DeleteDetector",
"guardduty:UpdateDetector",
"securityhub:DisableSecurityHub"
],
"Resource":[
"*"
]
}
]
}



- D.

Answer: A

NEW QUESTION # 338
A company has multiple accounts in the AWS Cloud. Users in the developer account need to have access to specific resources in the production account.
What is the MOST secure way to provide this access?

- A. Create one IAM user in the production account. Grant the appropriate permissions to the resources that are needed. Share the password only with the users that need access.
- B. Create cross-account access with an IAM user account in the production account. Grant the appropriate permissions to this user account. Allow users in the developer account to use this user account to access the production resources.
- C. Create cross-account access with an IAM role in the production account. Grant the appropriate permissions to this role. Allow users in the developer account to assume this role to access the production resources.
- D. Create cross-account access with an IAM role in the developer account. Grant the appropriate permissions to this role. Allow users in the developer account to assume this role to access the production resources.

Answer: C

Explanation:
https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

NEW QUESTION # 339
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 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.
- B. 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.
- C. Deploy the Lambda functions to a private subnet in the VPC. Create an S3 gateway endpoint to access the S3 service.
- D. Deploy the Lambda functions to a private subnet in the VPC. Configure the Lambda functions to access the S3 service through the NAT gateway.

Answer: C

Explanation:

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

NEW QUESTION # 340
.....

As we all know, passing an exam is not an easy thing for many candidates. They need time and energy to practice. SCS-C02 study materials will save your time with the skilled professional to compile them, and they are quite familiar with exam center. Therefore there is no need for you to research the SCS-C02 Study Materials by yourself. Furthermore, we use international recognition third party for your payment for SCS-C02 exam dumps, and your money and account safety can be guaranteed. If you find your interests haven't been guaranteed, you can ask for the refund.

What's more, part of that BraindumpsPrep SCS-C02 dumps now are free: https://drive.google.com/open?id=1mebL1sErgCuMq88PLhrEEYxeI3EoWOuY