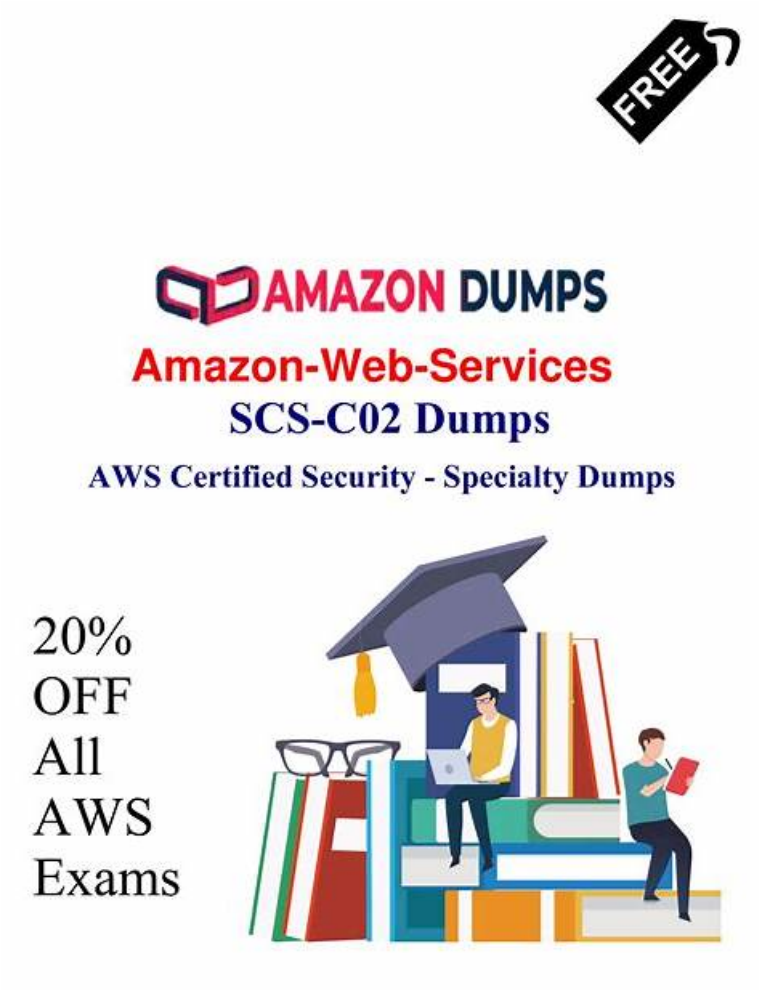
New SCS-C02 Test Camp, Free SCS-C02 Download Pdf



P.S. Free 2026 Amazon SCS-C02 dumps are available on Google Drive shared by Pass4Test: https://drive.google.com/open?id=1HY77Vf9kbKeK-VgB3wGaOGAkSuktAGkO

Thanks to modern technology, learning online gives people access to a wider range of knowledge, and people have got used to convenience of electronic equipment. As you can see, we are selling our SCS-C02 learning guide in the international market, thus there are three different versions of our SCS-C02 exam materials which are prepared to cater the different demands of various people. We can guarantee that our SCS-C02 Exam Materials are the best reviewing material. Concentrated all our energies on the study SCS-C02 learning guide we never change the goal of helping candidates pass the exam. Our SCS-C02 test questions' quality is guaranteed by our experts' hard work. So what are you waiting for? Just choose our SCS-C02 exam materials, and you won't be regret.

Amazon SCS-C02 Exam Syllabus Topics:

Topic	Details
Topic 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.

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	• 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 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.

One of the Best Ways to Prepare For the SCS-C02 AWS Certified Security - Specialty

Our SCS-C02 study guide provides free trial services, so that you can gain some information about our study contents, topics and how to make full use of the software before purchasing. It's a good way for you to choose what kind of SCS-C02 test prep is suitable and make the right choice to avoid unnecessary waste. Besides, if you have any trouble in the purchasing SCS-C02 practice torrent or trail process, you can contact us immediately and we will provide professional experts to help you online.

Amazon AWS Certified Security - Specialty Sample Questions (Q142-Q147):

NEW QUESTION # 142
A company has implemented IAM WAF and Amazon CloudFront for an application. The application runs on Amazon EC2 instances that are part of an Auto Scaling group. The Auto Scaling group is behind an Application Load Balancer (ALB).
The IAM WAF web ACL uses an IAM Managed Rules rule group and is associated with the CloudFront distribution. CloudFront receives the request from IAM WAF and then uses the ALB as the distribution's origin.
During a security review, a security engineer discovers that the infrastructure is susceptible to a large, layer 7 DDoS attack.
How can the security engineer improve the security at the edge of the solution to defend against this type of attack?

- A. Configure the CloudFront distribution to use IAM WAF as its origin instead of the ALB.
- B. Configure the IAM WAF web ACL so that the web ACL has more capacity units to process all IAM WAF rules faster.
- C. Configure IAM WAF with a rate-based rule that imposes a rate limit that automatically blocks requests when the rate limit is exceeded.
- D. Configure the CloudFront distribution to use the Lambda@Edge feature. Create an IAM Lambda function that imposes a rate limit on CloudFront viewer requests. Block the request if the rate limit is exceeded.

Answer: C

Explanation:
Explanation
To improve the security at the edge of the solution to defend against a large, layer 7 DDoS attack, the security engineer should do the following:
Configure AWS WAF with a rate-based rule that imposes a rate limit that automatically blocks requests when the rate limit is exceeded. This allows the security engineer to use a rule that tracks the number of requests from a single IP address and blocks subsequent requests if they exceed a specified threshold within a specified time period.

NEW QUESTION # 143
An AWS account includes two S3 buckets: bucketl and bucket2. The bucket2 does not have a policy defined, but bucketl has the following bucket policy:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": { "AWS":"arn:aws:iam::123456789012:user/alice" },
         "Action": "s3:*",
         "Resource": ["arn:aws:s3:::bucket1","arn:aws:s3:::bucket1/*"]
      }
   ]
}
```

In addition, the same account has an 1AM User named "alice", with the following 1AM policy.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": "s3:*",
         "Resource": ["arn:aws:s3:::bucket2","arn:aws:s3:::bucket2/*"]
      }
   ]
}
```

Which buckets can user "alice" access?

- A. bucketl only
- B. bucket2 only
- C. Neither bucketl nor bucket2
- D. Both bucketl and bucket2

Answer: D

Explanation:
Understanding the IAM Policy:
The IAM useralicehas an explicit permission in the IAM policy to perform alls3:*actions on bothbucket1andbucket2resources.
This grants useralicefull access to both buckets from the IAM policy perspective.
Bucket Policy for bucket1:
The bucket policy forbucket1explicitly grants useralicefull access to this bucket.
This policy reinforces the permissions provided by the IAM policy.
Bucket Policy for bucket2:
bucket2does not have a bucket policy defined.
In the absence of a bucket policy, the permissions fall back to the IAM policy.
Effective Permissions:
Since the IAM policy grants access to both buckets, and there are no conflicting explicit deny statements, useralicecan access bothbucket1andbucket2.
IAM Policies and Bucket Policies
Evaluating Access with S3 Policies

NEW QUESTION # 144
A company wants to ensure that its IAM resources can be launched only in the us-east-1 and us-west-2 Regions.
What is the MOST operationally efficient solution that will prevent developers from launching Amazon EC2 instances in other Regions?

- A. Provision EC2 resources by using IAM Cloud Formation templates through IAM CodePipeline. Allow only the values of us-east-1 and us-west-2 in the IAM CloudFormation template's parameters.
- B. Enable Amazon GuardDuty in all Regions. Create alerts to detect unauthorized activity outside us-east-1 and us-west-2.
- C. Create an IAM Config rule to prevent unauthorized activity outside us-east-1 and us-west-2.
- D. Use an organization in IAM Organizations. Attach an SCP that allows all actions when the IAM: Requested Region condition key is either us-east-1 or us-west-2. Delete the FullIAMAccess policy.

Answer: A

NEW QUESTION # 145
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. "NumericLessThan" : { "MaxSessionDuration " : "7200"}
- C. "NumericLessThan" : { " aws : Multi FactorAuthAge" : "7200"}
- D. "Bool " : " aws : Multi FactorAuthPresent": "true" }
- E. "NumericGreaterThan" : { " aws : MultiFactorAuthAge " : "7200"

Answer: C,D

Explanation:
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 access the 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 a role, but it cannot be used as a condition in a policy2.

NEW QUESTION # 146
A company runs workloads on Amazon EC2 instances. The company needs to continually scan the EC2 instances for software vulnerabilities and unintended network exposure.
Which solution will meet these requirements?

- A. Use Amazon Inspector. Enable the Malware Protection feature.
- B. Use Amazon Inspector. Set the scan mode to hybrid scanning.
- C. Use Amazon GuardDuty. Enable the Malware Protection feature.
- D. Use Amazon GuardDuty. Enable the Runtime Monitoring feature.

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Amazon Inspector offers automated, continuous vulnerability scanning for Amazon EC2 instances. The new version includes Malware Protection, which scans for malicious software as part of its inspection process.
This capability enables both detection of software vulnerabilities and malicious activity (like viruses or rootkits), thus covering both parts of the requirement: vulnerabilities and unintended network exposure.
This falls under Infrastructure Security and aligns with recommended practices for securing compute resources on AWS.

NEW QUESTION # 147
.....

If you are really not sure which version you like best, you can also apply for multiple trial versions of our SCS-C02 exam questions. We want our customers to make sensible decisions and stick to them. SCS-C02 study engine can be developed to today, and the principle of customer first is a very important factor. SCS-C02 Training Materials really hope to stand with you, learn together and grow together.