Amazon SCS-C02 Exam Questions For Greatest Achievement [Updated 2025]

DOWNLOAD the newest Dumps4PDF SCS-C02 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1hRg-t2IPrgeUFp28V91VgLairzVZD2e_

The modern world is becoming more and more competitive and if you are not ready for it then you will be not more valuable for job providers. Be smart in your career decision and enroll in AWS Certified Security - Specialty SCS-C02 Certification Exam and learn new and in demands skills. Dumps4PDF with AWS Certified Security - Specialty SCS-C02 exam questions and answers.

Amazon SCS-C02 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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.
Topic 3	• 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.
Topic 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.

>> Latest SCS-C02 Learning Material <<

VCE Amazon SCS-C02 Exam Simulator & SCS-C02 Test Questions Fee

Compared with companies that offer a poor level of customer service, our SCS-C02 exam questions have over 98 percent of chance to help you achieve success. Up to now, we have had thousands of letters and various feedbacks from satisfied customers

who are all faithful fans of our SCS-C02 Study Guide, and the number of them is keeping growing. So our SCS-C02 practice materials are the clear performance and manifestation of our sincerity. You really should have a try on our SCS-C02 exam dumps!

Amazon AWS Certified Security - Specialty Sample Questions (Q162-Q167):

NEW QUESTION # 162
A company used a lift-and-shift approach to migrate from its on-premises data centers to the AWS Cloud. The company migrated on-premises VMs to Amazon EC2 instances. Now the company wants to replace some of components that are running on the EC2 instances with managed AWS services that provide similar functionality.
Initially, the company will transition from load balancer software that runs on EC2 instances to AWS Elastic Load Balancers. A security engineer must ensure that after this transition, all the load balancer logs are centralized and searchable for auditing. The security engineer must also ensure that metrics are generated to show which ciphers are in use.
Which solution will meet these requirements?

- A. Create an Amazon CloudWatch Logs log group. Configure the load balancers to send logs to the log group. Use the CloudWatch Logs console to search the logs. Create CloudWatch Logs filters on the logs for the required metrics.
- B. Create an Amazon CloudWatch Logs log group. Configure the load balancers to send logs to the log group. Use the AWS Management Console to search the logs. Create Amazon Athena queries for the required metrics. Publish the metrics to Amazon CloudWatch.
- C. Create an Amazon S3 bucket. Configure the load balancers to send logs to the S3 bucket. Use Amazon Athena to search the logs that are in the S3 bucket. Create Amazon CloudWatch filters on the S3 log files for the required metrics.
- D. Create an Amazon S3 bucket. Configure the load balancers to send logs to the S3 bucket. Use Amazon Athena to search the logs that are in the S3 bucket. Create Athena queries for the required metrics. Publish the metrics to Amazon CloudWatch.

Answer: D

Explanation:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/add_custom_widget_sample s.html

NEW QUESTION # 163
For compliance reasons a Security Engineer must produce a weekly report that lists any instance that does not have the latest approved patches applied. The Engineer must also ensure that no system goes more than 30 days without the latest approved updates being applied What would the MOST efficient way to achieve these goals?

- A. Examine IAM CloudTrail togs to determine whether any instances have not restarted in the last 30 days, and redeploy those instances
- B. Configure Amazon EC2 Systems Manager to report on instance patch compliance and enforce updates during the defined maintenance windows
- C. Use Amazon inspector to determine which systems do not have the latest patches applied, and after 30 days, redeploy those instances with the latest AMI version
- D. Update the AMIs with the latest approved patches and redeploy each instance during the defined maintenance window

Answer: B

Explanation:
Explanation
Amazon EC2 Systems Manager is a service that helps you automatically collect software inventory, apply OS patches, create system images, and configure Windows and Linux operating systems3. You can use Systems Manager to report on instance patch compliance and enforce updates during the defined maintenance windows4. The other options are either inefficient or not feasible for achieving the goals.

NEW QUESTION # 164
An ecommerce website was down for 1 hour following a DDoS attack. Users were unable to connect to the website during the attack period. The ecommerce company's security team is worried about future potential attacks and wants to prepare for such events. The company needs to minimize downtime in its response to similar attacks in the future.
Which steps would help achieve this? (Select TWO.)

- A. Enable Amazon GuardDuty to automatically monitor for malicious activity and block unauthorized access.

- B. Set up an Amazon EventBridge rule to monitor the AWS CloudTrail events in real time, use AWS Config rules to audit the configuration, and use AWS Systems Manager for remediation.
- C. Use AWS WAF to create rules to respond to such attacks.
- D. Subscribe to AWS Shield Advanced and reach out to AWS Support in the event of an attack.
- E. Use VPC Flow Logs to monitor network traffic and an AWS Lambda function to automatically block an attacker's IP using security groups.

Answer: C,D

NEW QUESTION # 165
An AWS account administrator created an IAM group and applied the following managed policy to require that each individual user authenticate using multi-factor authentication:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*"
        },
        {
            "Sid": "BlockAnyAccessUnlessSignedInWithMFA",
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": false
                }
            }
        }
    ]
}
```

After implementing the policy, the administrator receives reports that users are unable to perform Amazon EC2 commands using the AWS CLI.
What should the administrator do to resolve this problem while still enforcing multi-factor authentication?

- A. Change the value of aws:MultiFactorAuthPresent to true.
- B. Instruct users to run the aws sts get-session-token CLI command and pass the multi-factor authentication --serial-number and --token-code parameters. Use these resulting values to make API/CLI calls.
- C. Create a role and enforce multi-factor authentication in the role trust policy. Instruct users to run the sts assume-role CLI command and pass --serial-number and --token-code parameters. Store the resulting values in environment variables. Add sts:AssumeRole to NotAction in the policy.
- D. Implement federated API/CLI access using SAML 2.0, then configure the identity provider to enforce multi-factor authentication.

Answer: B

Explanation:
The correct answer is B. Instruct users to run the aws sts get-session-token CLI command and pass the multi-factor authentication --serial-number and --token-code parameters. Use these resulting values to make API/CLI calls.
According to the AWS documentation1, the aws sts get-session-token CLI command returns a set of temporary credentials for an AWS account or IAM user. The credentials consist of an access key ID, a secret access key, and a security token. These credentials are valid for the specified duration only. The session duration for IAM users can be between 15 minutes and 36 hours, with a default of 12 hours.

You can use the --serial-number and --token-code parameters to provide the MFA device serial number and the MFA code from the device. The MFA device must be associated with the user who is making the get-session-token call. If you do not provide these parameters when your IAM user or role has a policy that requires MFA, you will receive an Access Denied error.
The temporary security credentials that are returned by the get-session-token command can then be used to make subsequent API or CLI calls that require MFA authentication. You can use environment variables or a profile in your AWS CLI configuration file to specify the temporary credentials.
Therefore, this solution will resolve the problem of users being unable to perform EC2 commands using the AWS CLI, while still enforcing MFA.
The other options are incorrect because:
* A. Changing the value of aws:MultiFactorAuthPresent to true will not work, because this is a condition key that is evaluated by AWS when a request is made. You cannot set this value manually in your policy or request. You must provide valid MFA information to AWS for this condition key to be true.
* C. Implementing federated API/CLI access using SAML 2.0 may work, but it requires more operational effort than using the get-session-token command. You would need to configure a SAML identity provider and trust relationship with AWS, and use a custom SAML client to request temporary
* credentials from AWS STS. This solution may also introduce additional security risks if the identity provider is compromised.
* D. Creating a role and enforcing MFA in the role trust policy may work, but it also requires more operational effort than using the get-session-token command. You would need to create a role for each user or group that needs to perform EC2 commands, and specify a trust policy that requires MFA. You would also need to grant the users permission to assume the role, and instruct them to use the sts assume-role command instead of the get-session-token command.
References:
1: get-session-token - AWS CLI Command Reference

NEW QUESTION # 166
A company has configured a gateway VPC endpoint in a VPC. Only Amazon EC2 instances that reside in a single subnet in the VPC can use the endpoint The company has modified the route table for this single subnet to route traffic to Amazon S3 through the gateway VPC endpoint. The VPC provides internet access through an internet gateway.
A security engineer attempts to use instance profile credentials from an EC2 instance to retrieve an object from the S3 bucket, but the attempt fails. The security engineer verifies that the EC2 instance has an 1AM instance profile with the correct permissions to access the S3 bucket and to retrieve objects. The security engineer also verifies that the S3 bucket policy is allowing access properly. Additionally, the security engineer verifies that the EC2 instance's security group and the subnet's network ACLs allow the communication.
What else should the security engineer check to determine why the request from the EC2 instance is failing?

- A. Verify that the VPC endpoint policy is allowing access to Amazon S3.
- B. Verify that the internet gateway is allowing traffic to Amazon S3.
- C. Verify that the VPC endpoint's security group does not have an explicit inbound deny rule for the EC2 instance.
- D. Verify that the EC2 instance's security group does not have an implicit inbound deny rule for Amazon S3.

Answer: A

NEW QUESTION # 167
.....

Download ✔ SCS-C02 □✔□ for free by simply entering ➡ www.pdfvce.com □□□ website □SCS-C02 Certification Test Questions

- SCS-C02 Latest Test Simulations □ SCS-C02 Valid Test Camp □ Key SCS-C02 Concepts □ Search for ☀ SCS-C02 □☀□ on □ www.passtestking.com □ immediately to obtain a free download □SCS-C02 Exam Exercise
- Reliable SCS-C02 Exam Blueprint □ Brain Dump SCS-C02 Free □ SCS-C02 Exam Material □ Search for [SCS-C02] and obtain a free download on □ www.pdfvce.com □ □SCS-C02 Lead2pass
- AWS Certified Security - Specialty pass guide: latest SCS-C02 exam prep collection □ Open website □ www.prep4pass.com □ and search for { SCS-C02 } for free download □SCS-C02 Lead2pass
- Reliable SCS-C02 Exam Preparation □ Test SCS-C02 Questions Vce □ SCS-C02 Lead2pass ✳ Search for □ SCS-C02 □ and download it for free on 「 www.pdfvce.com 」 website ↗ SCS-C02 Latest Test Simulations
- Trustable SCS-C02 – 100% Free Latest Learning Material | VCE SCS-C02 Exam Simulator ↘ Search for ➤ SCS-C02 □ and download it for free on ➽ www.getvalidtest.com □ website □SCS-C02 Exam Material
- SCS-C02 Reliable Exam Braindumps □ SCS-C02 Well Prep □ SCS-C02 Valid Test Camp □ Search for （ SCS-C02 ） and easily obtain a free download on ☀ www.pdfvce.com □☀□ □SCS-C02 Well Prep
- Latest SCS-C02 Exam Labs □ SCS-C02 Exam Collection Pdf □ SCS-C02 Well Prep □ Easily obtain free download of ✔ SCS-C02 □✔□ by searching on ➠ www.actual4labs.com □ □SCS-C02 Exam Exercise
- www.61921c.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, daotao.wisebusiness.edu.vn, 114.115.238.41, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, academy.quantalgos.in, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

BONUS!!! Download part of Dumps4PDF SCS-C02 dumps for free: https://drive.google.com/open?id=1hRg-t2IPrgeUFp28V91VgLairzVZD2e_