Free PDF 2026 Perfect Amazon SCS-C02: New AWS Certified Security - Specialty Dumps Pdf

DOWNLOAD the newest Real4dumps SCS-C02 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1OxcgzgulbAogqJZ9PVTkXS4d0lYOAKG-

Our SCS-C02 study quiz boosts many advantages and it is your best choice to prepare for the test. Our SCS-C02 learning prep is compiled by our first-rate expert team and linked closely with the real exam. And our SCS-C02 training materials provide three versions and multiple functions to make the learners have no learning obstacles. The passing rate of our SCS-C02 Guide materials is high and you don't need to worry that you have spent money but can't pass the test.

We provide you with two kinds of consulting channels if you are confused about some questions on our SCS-C02 study materials. You can email us or contact our online customer service. We will reply you as soon as possible. You are free to ask questions about SCS-C02 training prep at any time since that we are working 24/7 online. Our staff is really very patient and friendly. They are waiting to give you the most professional suggestions on our SCS-C02 exam questions.

>> New SCS-C02 Dumps Pdf <<

SCS-C02 Reliable Dumps Pdf, Valid SCS-C02 Exam Bootcamp

Our product boosts many merits and high passing rate. Our products have 3 versions and we provide free update of the Amazon exam torrent to you. If you are the old client you can enjoy the discounts. Most important of all, as long as we have compiled a new version of the SCS-C02 Exam Questions, we will send the latest version of our Amazon exam questions to our customers for free during the whole year after purchasing. Our product can improve your stocks of knowledge and your abilities in some area and help you gain the success in your career.

Amazon SCS-C02 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 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	• 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 5	• 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.

Amazon AWS Certified Security - Specialty Sample Questions (Q241-Q246):

NEW QUESTION # 241
An audit determined that a company's Amazon EC2 instance security group violated company policy by allowing unrestricted incoming SSH traffic. A security engineer must implement a near-real-time monitoring and alerting solution that will notify administrators of such violations.
Which solution meets these requirements with the MOST operational efficiency?

- A. Create a recurring Amazon Inspector assessment run that runs every day and uses the Network Reachability package. Create an Amazon CloudWatch rule that invokes an IAM Lambda function when an assessment run starts. Configure the Lambda function to retrieve and evaluate the assessment run report when it completes. Configure the Lambda function also to publish an Amazon Simple Notification Service (Amazon SNS) notification if there are any violations for unrestricted incoming SSH traffic.
- B. Create a recurring Amazon Inspector assessment run that runs every day and uses the Security Best Practices package. Create an Amazon CloudWatch rule that invokes an IAM Lambda function when an assessment run starts. Configure the Lambda function to retrieve and evaluate the assessment run report when it completes. Configure the Lambda function also to publish an Amazon Simple Notification Service (Amazon SNS) notification if there are any violations for unrestricted incoming SSH traffic.
- C. Configure VPC Flow Logs for the VPC. and specify an Amazon CloudWatch Logs group. Subscribe the CloudWatch Logs group to an IAM Lambda function that parses new log entries, detects successful connections on port 22, and publishes a notification through Amazon Simple Notification Service (Amazon SNS).
- D. Use the restricted-ssh IAM Config managed rule that is invoked by security group configuration changes that are not compliant. Use the IAM Config remediation feature to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic.

Answer: D

Explanation:
The most operationally efficient solution to implement a near-real-time monitoring and alerting solution that will notify administrators of security group violations is to use the restricted-ssh AWS Config managed rule that is invoked by security group configuration changes that are not compliant. This rule checks whether security groups that are in use have inbound rules that allow unrestricted SSH traffic. If a violation is detected, AWS Config can use the remediation feature to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic.
Option A is incorrect because creating a recurring Amazon Inspector assessment run that uses the Network Reachability package is not operationally efficient, as it requires setting up an assessment target and template, running the assessment every day, and invoking a Lambda function to retrieve and evaluate the assessment report. It also does not provide near-real-time monitoring and alerting, as it depends on the frequency and duration of the assessment run.
Option C is incorrect because configuring VPC Flow Logs for the VPC and specifying an Amazon CloudWatch Logs group is not operationally efficient, as it requires creating a log group and stream, enabling VPC Flow Logs for each subnet or network interface,

and subscribing a Lambda function to parse and analyze the log entries. It also does not provide proactive monitoring and alerting, as it only detects successful connections on port 22 after they have occurred.
Option D is incorrect because creating a recurring Amazon Inspector assessment run that uses the Security Best Practices package is not operationally efficient, for the same reasons as option A. It also does not provide specific monitoring and alerting for security group violations, as it covers a broader range of security issues. References:
* [AWS Config Rules]
* [AWS Config Remediation]
* [Amazon Inspector]
* [VPC Flow Logs]

NEW QUESTION # 242
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. Implement federated API/CLI access using SAML 2.0, then configure the identity provider to enforce multi-factor authentication.
- C. 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.
- D. 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.

Answer: C

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 # 243
A Security Engineer is working with a Product team building a web application on AWS. The application uses Amazon S3 to host the static content, Amazon API Gateway to provide RESTful services; and Amazon DynamoDB as the backend data store. The users already exist in a directory that is exposed through a SAML identity provider.
Which combination of the following actions should the Engineer take to enable users to be authenticated into the web application and call APIs? (Choose three.)

- A. Configure an Amazon Cognito identity pool to integrate with social login providers.
- B. Update DynamoDB to store the user email addresses and passwords.
- C. Update API Gateway to use a COGNITO_USER_POOLS authorizer.
- D. Configure a SAML identity provider in Amazon Cognito to map attributes to the Amazon Cognito user pool attributes.
- E. Configure the SAML identity provider to add the Amazon Cognito user pool as a relying party.
- F. Create a custom authorization service using AWS Lambda.

Answer: C,D,E

Explanation:
The combination of the following actions should the Engineer take to enable users to be authenticated into the web application and call APIs are:
B) Configure a SAML identity provider in Amazon Cognito to map attributes to the Amazon Cognito user pool attributes. This is a necessary step to federate the existing users from the SAML identity provider to the Amazon Cognito user pool, which will be used for authentication and authorization1.
C) Configure the SAML identity provider to add the Amazon Cognito user pool as a relying party. This is a necessary step to establish a trust relationship between the SAML identity provider and the Amazon Cognito user pool, which will allow the users to sign in using their existing credentials2.
F) Update API Gateway to use a COGNITO_USER_POOLS authorizer. This is a necessary step to enable API Gateway to use the Amazon Cognito user pool as an authorizer for the RESTful services, which will validate the identity or access tokens that are issued by Amazon Cognito when a user signs in successfully3.
The other options are incorrect because:
A) Creating a custom authorization service using AWS Lambda is not a necessary step, because Amazon Cognito user pools can provide built-in authorization features, such as scopes and groups, that can be used to control access to API resources4.
D) Configuring an Amazon Cognito identity pool to integrate with social login providers is not a necessary step, because the users already exist in a directory that is exposed through a SAML identity provider, and there is no requirement to support social login providers5.

E) Updating DynamoDB to store the user email addresses and passwords is not a necessary step, because the user credentials are already stored in the SAML identity provider, and there is no need to duplicate them in DynamoDB6.
Reference:
1: Using Tokens with User Pools 2: Adding SAML Identity Providers to a User Pool 3: Control Access to a REST API Using Amazon Cognito User Pools as Authorizer 4: API Authorization with Resource Servers and OAuth 2.0 Scopes 5: Using Identity Pools (Federated Identities) 6: Amazon DynamoDB

NEW QUESTION # 244
A company is using AWS Organizations to create OUs for its accounts. The company has more than 20 accounts that are all part of the OUs. A security engineer must implement a solution to ensure that no account can stop to file delivery to AWS CloudTrail.
Which solution will meet this requirement?

- A. Use AWS Systems Manager to ensure that CloudTrail is always turned on.
- B. Create an SCP that includes a Deny rule tor the cloudtrail. StopLogging action Apply the SCP to all accounts in the OUs.
- C. Create an SCP that includes an Allow rule for the cloudtrail. StopLogging action Apply the SCP to all accounts in the OUs.
- D. Use the --is-multi-region-trail option while running the create-trail command to ensure that logs are configured across all AWS Regions.

Answer: B

Explanation:
Explanation
This SCP prevents users or roles in any affected account from disabling a CloudTrail log, either directly as a command or through the console. https://asecure.cloud/a/scp_cloudtrail/

NEW QUESTION # 245
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 assessment reports in the Audit Manager console to find InstanceCredentialExfiltration events.
- C. Review CloudWatch logs for GetSessionToken API calls to AWS Security Token Service (AWS STS) that come from an account ID from outside the company.
- D. Review CloudTrail logs for GetSessionToken API calls to AWS Security Token Service (AWS STS) that come from an acount ID from outside the company.

Answer: A

Explanation:
The correct answer is A because 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 differentAWS account than the one that owns the instance1. 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 credentials2.
The other options are incorrect because they do not provide the information needed to determine if the credentials were used to access the company's resources from an external account. Option B is incorrect because Audit Manager does not generate InstanceCredentialExfiltration events. Audit Manager is a service that helpsyou continuously audit your AWS usage to simplify how you assess risk and compliance with regulations and industry standards3. Option C is incorrect because CloudTrail logs do not show the account ID of the caller for GetSessionToken API calls to AWS STS. CloudTrail logs show the account ID of the identity whose credentials were used to call the API4. Option D is incorrect because CloudWatch logs do not show the GetSessionToken API calls to AWS STS by default. CloudWatch logs can show the API calls made by AWS Lambda functions, Amazon API Gateway, and other AWS services that integrate with CloudWatch5.
Reference: InstanceCredentialExfiltration, Amazon GuardDuty Enhances Detection of EC2 Instance Credential Exfiltration, What Is AWS Audit Manager?, Logging AWS STS API Calls with AWS CloudTrail, What IsAmazon CloudWatch Logs?

NEW QUESTION # 246
.....

The goal of SCS-C02 preparation material is to help applicants prepare for the AWS Certified Security - Specialty certification exam by providing them with the Actual SCS-C02 Exam Questions they need to pass the exam. This AWS Certified Security - Specialty (SCS-C02) study material is in the form of practice tests and SCS-C02 PDF that thoroughly covers the content of the test.

SCS-C02 Reliable Dumps Pdf: https://www.real4dumps.com/SCS-C02_examcollection.html

- SCS-C02 Exam Quiz □ SCS-C02 Hot Questions □ Exam SCS-C02 Price □ 【 www.pdfdumps.com 】 is best website to obtain [SCS-C02] for free download □SCS-C02 New Braindumps Sheet
- Test SCS-C02 Assessment □ Test SCS-C02 Assessment □ SCS-C02 Exam Quiz □ Easily obtain ▹ SCS-C02 ◃ for free download through （ www.pdfvce.com ） □SCS-C02 Hot Questions
- Updated New SCS-C02 Dumps Pdf | Amazing Pass Rate For SCS-C02 Exam | Marvelous SCS-C02: AWS Certified Security - Specialty □ Download （ SCS-C02 ） for free by simply entering ➥ www.examcollectionpass.com □ website □SCS-C02 Exam Quiz
- Updated New SCS-C02 Dumps Pdf | Amazing Pass Rate For SCS-C02 Exam | Marvelous SCS-C02: AWS Certified Security - Specialty □ Go to website □ www.pdfvce.com □ open and search for □ SCS-C02 □ to download for free □Latest Test SCS-C02 Discount
- Latest Amazon New SCS-C02 Dumps Pdf and High Hit Rate SCS-C02 Reliable Dumps Pdf □ Search for { SCS-C02 } and download it for free on ⇛ www.prepawayexam.com ⇚ website □Certification SCS-C02 Book Torrent
- Latest Test SCS-C02 Discount □ SCS-C02 Reliable Study Guide □ Prep SCS-C02 Guide □ ➠ www.pdfvce.com □ is best website to obtain □ SCS-C02 □ for free download □Pass SCS-C02 Guaranteed
- SCS-C02 Valid Dumps Free □ Certification SCS-C02 Book Torrent □ Pass SCS-C02 Guaranteed □ Download ☀ SCS-C02 □☀□ for free by simply entering ▸ www.examcollectionpass.com ◂ website □SCS-C02 Valid Exam Materials
- SCS-C02 - AWS Certified Security - Specialty Authoritative New Dumps Pdf □ Search for ☀ SCS-C02 □☀□ and easily obtain a free download on □ www.pdfvce.com □ □Pass4sure SCS-C02 Dumps Pdf
- Amazon New SCS-C02 Dumps Pdf: AWS Certified Security - Specialty - www.examcollectionpass.com Gives Warm Service - Excellent Reliable Dumps Pdf □ ▹ www.examcollectionpass.com ◃ is best website to obtain 【 SCS-C02 】 for free download □SCS-C02 Valid Exam Materials
- 100% Pass 2026 Amazon SCS-C02 Fantastic New Dumps Pdf □ Search for 「 SCS-C02 」 and easily obtain a free download on ▸ www.pdfvce.com ◂ □Pass4sure SCS-C02 Dumps Pdf
- Pass SCS-C02 Guaranteed □ Exam SCS-C02 Price □ SCS-C02 Dumps Collection □ Search for ✔ SCS-C02 □✔□ on { www.practicevce.com } immediately to obtain a free download □SCS-C02 Exam Quiz
- pennycdrq165452.mdkblog.com, todaybookmarks.com, 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, umarftng809210.shoutmyblog.com, www.dibiz.com, graysontiwy988182.wikilima.com, tamzinsgtb007768.tokka-blog.com, berthacpok180559.wikinstructions.com, heidirgqs090394.ktwiki.com, siobhanhehd756752.wikiconversation.com, Disposable vapes

BTW, DOWNLOAD part of Real4dumps SCS-C02 dumps from Cloud Storage: https://drive.google.com/open?id=1OxcgzgulbAogqJZ9PVTkXS4d0lYOAKG-