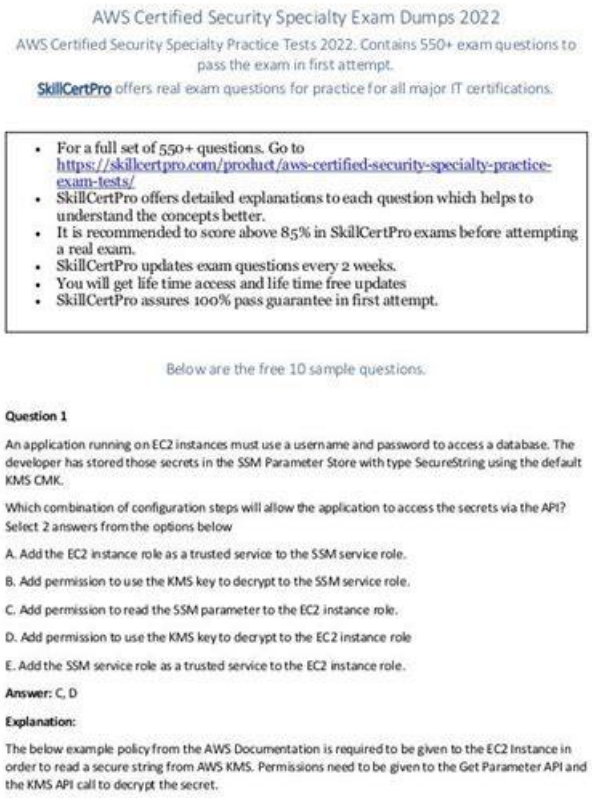
Free PDF Perfect Amazon - SCS-C03 - Test AWS Certified Security - Specialty Preparation



AWS Certified Security Specialty Exam Dumps 2022

AWS Certified Security Specialty Practice Tests 2022. Contains 550+ exam questions to pass the exam in first attempt.

SkillCertPro offers real exam questions for practice for all major IT certifications.

- For a full set of 550+ questions. Go to https://skillcertpro.com/product/aws-certified-security-specialty-practice-exam-tests/
- SkillCertPro offers detailed explanations to each question which helps to understand the concepts better.
- It is recommended to score above 85% in SkillCertPro exams before attempting a real exam.
- SkillCertPro updates exam questions every 2 weeks.
- You will get life time access and life time free updates
- SkillCertPro assures 100% pass guarantee in first attempt.

Below are the free 10 sample questions.

Question 1

An application running on EC2 instances must use a username and password to access a database. The developer has stored those secrets in the SSM Parameter Store with type SecureString using the default KMS CMK.

Which combination of configuration steps will allow the application to access the secrets via the API? Select 2 answers from the options below

A. Add the EC2 instance role as a trusted service to the SSM service role.

B. Add permission to use the KMS key to decrypt to the SSM service role.

C. Add permission to read the SSM parameter to the EC2 instance role.

D. Add permission to use the KMS key to decrypt to the EC2 instance role

E. Add the SSM service role as a trusted service to the EC2 instance role.

Answer: C, D

Explanation:

The below example policy from the AWS Documentation is required to be given to the EC2 Instance in order to read a secure string from AWS KMS. Permissions need to be given to the Get Parameter API and the KMS API call to decrypt the secret.

P.S. Free 2026 Amazon SCS-C03 dumps are available on Google Drive shared by TestKingIT: https://drive.google.com/open?id=1UtWmvOtymfey4ViKGok2muu-GrJieCCv

TestKingIT AWS Certified Security - Specialty (SCS-C03) PDF exam questions file is portable and accessible on laptops, tablets, and smartphones. This pdf contains test questions compiled by experts. Answers to these pdf questions are correct and cover each section of the examination. You can even use this format of AWS Certified Security - Specialty questions without restrictions of place and time. This Amazon SCS-C03 Pdf Format is printable to read real questions manually. We update our pdf questions collection regularly to match the updates of the Amazon SCS-C03 real exam.

Amazon SCS-C03 Exam Syllabus Topics:

Section	Weight	Objectives
Topic 1: Management, Governance and Compliance	14%	- Governance frameworks • 1. AWS Organizations and SCPs • 2. Multi-account security strategy - Compliance and auditing • 1. Security best practices alignment (CIS, NIST) • 2. AWS Artifact compliance reports

Topic 2: Data Protection	18%	- Encryption and key management • 1. Encryption at rest and in transit • 2. AWS KMS key management - Data security services • 1. Amazon S3 security controls • 2. Secrets Manager and Parameter Store
Topic 3: Threat Detection and Incident Response	14%	- Detection mechanisms • 1. Amazon GuardDuty threat detection • 2. AWS Security Hub findings aggregation - Incident response procedures • 1. Identify and investigate security incidents in AWS environments • 2. Automate response using AWS services (Lambda, CloudWatch, EventBridge)
Topic 4: Identity and Access Management	16%	- Federation and access control • 1. Federated identity with SAML/OIDC • 2. IAM Identity Center (SSO) - AWS IAM fundamentals • 1. Least privilege access design • 2. Users, groups, roles, and policies
Topic 5: Logging and Monitoring	18%	- Monitoring and alerting • 1. Amazon CloudWatch metrics and alarms • 2. Centralized security monitoring strategies - Audit logging • 1. AWS Config configuration tracking • 2. AWS CloudTrail logging and analysis
Topic 6: Infrastructure Security	20%	- Compute security • 1. EC2 instance hardening • 2. Container security (ECS/EKS basics) - Network security • 1. Security groups and NACLs • 2. VPC design and segmentation

3 Formats of Amazon SCS-C03 Dumps that Suit your Study Style

SCS-C03 exam dumps are famous for high-quality, since we have a professional team to collect and research the first-hand information. We have reliable channel to ensure you that SCS-C03 exam braindumps you receive is the latest information of the exam. We are strict with the quality and answers of SCS-C03 Exam Materials, we can guarantee you that what you receive are the best and most effective. In addition, online and offline chat service stuff are available, and if you have any questions for SCS-C03 exam dumps, you can consult us.

Amazon AWS Certified Security - Specialty Sample Questions (Q126-Q131):

NEW QUESTION # 126
A company has an organization with all features enabled in AWS Organizations. In the management account, the company configures AWS IAM Identity Center for the organization in the eu-west-2 Region. The company configures IAM Identity Center with a SAML-based identity provider.
The company needs to configure an AWS managed application that integrates with IAM Identity Center in a new AWS account in the us-east-1 Region. Most of the users that will authenticate to the AWS managed application are external third-party users who cannot be added to the company's identity provider.
A security engineer needs to configure authentication for the third-party users. The solution must provide isolation from the company's identity provider.
Which solution will meet these requirements?

- A. Deploy Amazon Cognito into the new AWS account in us-east-1. Configure an identity pool for a SAML-based identity provider. Configure an IAM role that uses the sts:AssumeRole action to allow access to the AWS managed application from Amazon Cognito.
- B. Create a new identity provider for the third-party users. Configure a second identity source in IAM Identity Center in the organization's management account to use the new identity provider. Create a new permission set that gives access to the AWS managed application in the new account.
- C. Enable account instances in IAM Identity Center. Deploy an IAM Identity Center account instance in the new AWS account in us-east-1. Configure the AWS managed application to use the new instance. Configure users in the new account instance directory.
- D. Create a SAML identity provider in IAM in the management account that connects to the third-party users' identity provider. Create IAM roles in the management account that allow access to the AWS managed application.

Answer: C

Explanation:
IAM Identity Center account instances are designed for isolated deployments of supported AWS managed applications in a single AWS account. AWS documentation states that account instances should be used for isolated users who need applications in one account, and they remain bound to the account in which they are created. This matches the requirement:
third-party users cannot be added to the company's main IdP, and access must be isolated from the organization-level IAM Identity Center identity source. Amazon Cognito identity pools do not configure authentication for IAM Identity Center integrated AWS managed applications in this pattern. IAM SAML roles in the management account would not isolate the application account cleanly. IAM Identity Center supports one identity source per instance, so adding a second identity source to the organization instance is not the right design.

NEW QUESTION # 127
A company is using Amazon Elastic Container Service (Amazon ECS) to deploy an application that deals with sensitive data. During a recent security audit, the company identified a security issue in which Amazon RDS credentials were stored with the application code in the company ' s source code repository. A security engineer needs to develop a solution to ensure that database credentials are stored securely and rotated periodically. The credentials should be accessible to the application only. The engineer also needs to prevent database administrators from sharing database credentials as plaintext with other teammates. The solution must also minimize administrative overhead.
Which solution meets these requirements?

- A. Use AWS Secrets Manager to store database credentials. Use IAM roles for ECS tasks to restrict access to database credentials to specific containers only.
- B. Use the AWS Systems Manager Parameter Store to generate database credentials. Use an IAM profile for ECS tasks to restrict access to database credentials to specific containers only.
- C. Use AWS Secrets Manager to store database credentials. Use an IAM inline policy for ECS tasks to restrict access to database credentials to specific containers only.
- D. Use the AWS Systems Manager Parameter Store to store database credentials. Use IAM roles for ECS tasks to restrict access to database credentials to specific containers only.

Answer: A

Explanation:
AWS Secrets Manageris the AWS service designed to store secrets securely and to supportautomatic rotationon a schedule-commonly used for Amazon RDS credentials. Storing credentials in Secrets Manager removes them from source code, enables fine-

grained access control, and supports auditability of secret retrieval through CloudTrail. Rotation can be configured to periodically change the database password and update the stored secret automatically, minimizing operational overhead compared to manual rotation processes.
To ensure the credentials are accessibleonly to the application, the correct ECS pattern is to useIAM roles for tasks. A task role can be scoped to allow only secretsmanager:GetSecretValue (and related actions if needed) for the specific secret ARN. Only tasks running with that role can retrieve the secret at runtime, which prevents broad access. This also helps reduce the risk of database administrators sharing plaintext credentials, because the recommended operational model is that humans should not need direct access; the application retrieves the secret programmatically, and access can be limited to break-glass workflows if required.
Systems Manager Parameter Store can store encrypted parameters, but Secrets Manager provides stronger native secret lifecycle features (notably rotation) for databases. Inline policies (Option B) are not necessary; managed or attached policies on the task role achieve the same goal with cleaner administration.

NEW QUESTION # 128
A company has the following security policy for its Amazon Aurora MySQL databases for a single AWS account:
- Database storage must be encrypted at rest.
- Deletion protection must be enabled.
- Databases must not be publicly accessible.
- Database audit logs must be published to Amazon CloudWatch Logs.
A security engineer must implement a solution that continuously monitors all Aurora MySQL resources for compliance with this policy. The solution must be able to display a database's compliance state for each part of the policy at any time.
Which solution will meet these requirements?

- A. Enable AWS Security Hub. Create a configuration policy that includes the security requirements. Apply the configuration policy to all Aurora MySQL resources. View the compliance state in Security Hub.
- B. Enable AWS Audit Manager. Configure Audit Manager to use a custom framework that matches the security requirements. Create an assessment report to view the compliance state.
- C. Enable AWS Config. Implement AWS Config managed rules that monitor all Aurora MySQL resources for the security requirements. View the compliance state in the AWS Config dashboard.
- D. Create an Amazon EventBridge rule that runs when an Aurora MySQL resource is created or modified. Create an AWS Lambda function to verify the security requirements and to send the compliance state to a CloudWatch custom metric.

Answer: C

Explanation:
AWS Config is a fully managed service that provides continuous monitoring and evaluation of AWS resource configurations against desired configuration baselines. According to the AWS Certified Security - Specialty Official Study Guide, AWS Config is the primary service used to track configuration changes, evaluate compliance in near real time, and display compliance states for individual AWS resources.
AWS Config provides managed rules that directly map to the listed Aurora MySQL security requirements, including encryption at rest, public accessibility, deletion protection, and log exports to CloudWatch Logs. These managed rules continuously evaluate resources and mark them as compliant or noncompliant whenever a configuration change occurs.
The AWS Config dashboard enables security engineers to view per-resource and per-rule compliance states at any point in time, satisfying the requirement to display compliance status for each part of the policy.

NEW QUESTION # 129
A security engineer is asked to update an AWS CloudTrail log file prefix for an existing trail. When attempting to save the change in the CloudTrail console, the security engineer receives the following error message: "There is a problem with the bucket policy." What will enable the security engineer to save the change?

- A. Create a new trail with the updated log file prefix, and then delete the original trail.
- B. Update the existing bucket policy in the Amazon S3 console to allow the security engineer's principal to perform GetBucketPolicy, and then update the log file prefix in the CloudTrail console.
- C. Update the existing bucket policy in the Amazon S3 console to allow the security engineer's principal to perform PutBucketPolicy, and then update the log file prefix in the CloudTrail console.
- D. Update the existing bucket policy in the Amazon S3 console with the new log file prefix, and then update the log file prefix in the CloudTrail console.

Answer: D

Explanation:
CloudTrail must be allowed to deliver log files to the exact Amazon S3 bucket prefix configured for the trail. If the S3 bucket policy still references the old prefix, CloudTrail detects the mismatch and returns the bucket policy error. AWS documentation explicitly states that when adding, modifying, or removing a log file prefix for a bucket receiving CloudTrail logs, the bucket policy must be updated first with the matching prefix, and then the CloudTrail trail should be updated to use that same prefix. Creating a new trail is unnecessary. Granting PutBucketPolicy or GetBucketPolicy to the security engineer does not fix the CloudTrail service delivery path. The issue is the prefix value in the bucket policy.

NEW QUESTION # 130
A company in France uses Amazon Cognito with the Cognito Hosted UI as an identity broker for sign-in and sign-up processes. The company is marketing an application and expects that all the application ' s users will come from France. When the company launches the application, the company ' s security team observes fraudulent sign-ups for the application. Most of the fraudulent registrations are from users outside of France.
The security team needs a solution to perform custom validation at sign-up. Based on the results of the validation, the solution must accept or deny the registration request.
Which combination of steps will meet these requirements? (Select TWO.)

- A. Update the application ' s Amazon Cognito user pool to configure a geographic restriction setting.
- B. Use a geographic match rule statement to configure an AWS WAF web ACL. Associate the web ACL with the Amazon Cognito user pool.
- C. Use Amazon Cognito to configure a social identity provider (IdP) to validate the requests on the hosted UI.
- D. Create a pre sign-up AWS Lambda trigger. Associate the Amazon Cognito function with the Amazon Cognito user pool.
- E. Configure an app client for the application ' s Amazon Cognito user pool. Use the app client ID to validate the requests in the hosted UI.

Answer: B,D

Explanation:
To performcustom validation at sign-upand explicitlyaccept or denyregistrations, Amazon Cognito providesLambda triggers. APre sign-up triggerruns synchronously during the sign-up flow (including the Hosted UI) and can implement custom checks (for example, IP reputation checks, email/domain validation, velocity checks, allow/deny lists, or geo checks using an external service). Based on the trigger logic, the function can allow the sign-up to proceed or reject it, meeting the "custom validation" and "accept/deny" requirement directly.
Because the observed fraud largely originatesoutside France, adding a front-door geographic control reduces unwanted traffic before it reaches Cognito.AWS WAFsupportsGeo matchconditions in a web ACL to allow
/deny requests by country, which is a common mitigation for region-scoped applications. Associating a WAF web ACL to protect the Hosted UI endpoint helps block sign-up requests from non-French locations early, reducing fraud attempts and load.
The other options do not meet the requirement: Cognito user pools do not provide a native "geographic restriction setting" for sign-up (D), app client ID validation does not stop fraudulent sign-ups (C), and using a social IdP does not provide custom accept/deny validation for all sign-ups (E).

NEW QUESTION # 131
.....

www.pdfvce.com □ and search for ➥ SCS-C03 □ to download for free □New SCS-C03 Test Guide

- SCS-C03 Interactive EBook □ SCS-C03 Interactive EBook ❤□ Reliable Exam SCS-C03 Pass4sure □ Search for ➥ SCS-C03 □ and download it for free on 《 www.prep4sures.top 》 website □Related SCS-C03 Exams
- Reliable SCS-C03 Exam Simulator □ Related SCS-C03 Exams □ Reliable SCS-C03 Exam Simulator □ Search on 【 www.pdfvce.com 】 for ✔ SCS-C03 □✔□ to obtain exam materials for free download □Examcollection SCS-C03 Dumps Torrent
- Reliable SCS-C03 Exam Simulator □ Reliable SCS-C03 Exam Simulator □ New SCS-C03 Mock Exam □ Search for ➠ SCS-C03 □ and download it for free immediately on { www.pass4test.com } □Instant SCS-C03 Download
- SCS-C03 New Exam Bootcamp □ SCS-C03 Actual Test □ SCS-C03 Brain Dump Free □ Search for □ SCS-C03 □ and easily obtain a free download on ⇛ www.pdfvce.com ⇚ ↘Reliable SCS-C03 Exam Simulator
- Free PDF Test SCS-C03 Preparation | Latest Amazon Visual SCS-C03 Cert Exam: AWS Certified Security - Specialty □ Search for ➡ SCS-C03 □□□ and download exam materials for free through 【 www.vceengine.com 】 □Real SCS-C03 Dumps
- Examcollection SCS-C03 Dumps Torrent ☀ Instant SCS-C03 Download □ Instant SCS-C03 Download □ Search for ➡ SCS-C03 □□□ and download it for free immediately on 「 www.pdfvce.com 」 □Reliable SCS-C03 Exam Simulator
- Examcollection SCS-C03 Dumps Torrent □ Related SCS-C03 Exams □ Free SCS-C03 Test Questions □ Search for □ SCS-C03 □ and download it for free on 【 www.torrentvce.com 】 website ☣Reliable Exam SCS-C03 Pass4sure
- myportal.utt.edu.tt, 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, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, 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, www.stes.tyc.edu.tw, youemerge.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, Disposable vapes

P.S. Free & New SCS-C03 dumps are available on Google Drive shared by TestKingIT: https://drive.google.com/open?id=1UtWmvOtymfey4ViKGok2muu-GrJieCCv