SAP-C02 New Test Bootcamp | SAP-C02 Valid Torrent

2026 Latest ValidBraindumps SAP-C02 PDF Dumps and SAP-C02 Exam Engine Free Share: https://drive.google.com/open?id=1By-8sBhkLdppykYOfNjF83gNaHFjcU2d

To assimilate those useful knowledge better, many customers eager to have some kinds of practice materials worth practicing. All content is clear and easily understood in our SAP-C02 practice materials. They are accessible with reasonable prices and various versions for your option. All content are in compliance with regulations of the exam. As long as you are determined to succeed, our SAP-C02 Study Guide will be your best reliance

The ValidBraindumps product here is better, cheaper, higher quality and unlimited for all time; kiss the days of purchasing multiple Amazon braindumps repeatedly, or renewing SAP-C02 training courses because you ran out of time. Now you can learn SAP-C02 skills and theory at your own pace and anywhere you want with top of the SAP-C02 braindumps, you will find it's just like a pice a cake to pass SAP-C02exam.

>> SAP-C02 New Test Bootcamp <<

SAP-C02 Valid Torrent | Interactive SAP-C02 Practice Exam

ValidBraindumps is a rich-experienced website specialized in the Amazon dump torrent and real pdf dumps. These pdf study materials are concluded by our professional IT trainers who have a good knowledge of SAP-C02 Exam Questions torrent. They check the updating of vce braindumps every day to ensure the accuracy of SAP-C02 test questions and answers.

The SAP-C02 exam consists of multiple-choice and multiple-response questions that test your knowledge of AWS architecture, deployment, and management. SAP-C02 exam is administered by Pearson VUE and can be taken at any of their testing centers around the world. SAP-C02 Exam Fee is $300, and you will have 180 minutes to complete the exam.

Amazon AWS Certified Solutions Architect - Professional (SAP-C02) Sample Questions (Q452-Q457):

NEW QUESTION # 452
A company needs to use an AWS Transfer Family SFTP-enabled server with an Amazon S3 bucket to receive updates from a third-party data supplier. The data is encrypted with Pretty Good Privacy (PGP) encryption The company needs a solution that will automatically decrypt the data after the company receives the data A solutions architect will use a Transfer Family managed workflow The company has created an 1AM service role by using an 1AM policy that allows access to AWS Secrets Manager and the S3 bucket The role's trust relationship allows the transfer amazonaws com service to assume the rote What should the solutions architect do next to complete the solution for automatic decryption'?

- A. Store the PGP private key in Secrets Manager Add a nominal step in the Transfer Family managed workflow to decrypt files. Configure PGP decryption parameters in the nominal step Associate the workflow with the Transfer Family server
- B. Store the PGP public key in Secrets Manager Add an exception-handling step in the Transfer Family managed workflow

to decrypt files Configure PGP decryption parameters in the exception handler Associate the workflow with the SFTP user

- C. Store the PGP private key in Secrets Manager Add an exception-handling step in the Transfer Family managed workflow to decrypt files Configure PGP encryption parameters in the exception handler Associate the workflow with the SFTP user
- D. Store the PGP public key in Secrets Manager Add a nominal step in the Transfer Family managed workflow to decrypt files Configure PGP encryption parameters in the nominal step Associate the workflow with the Transfer Family server

Answer: A

Explanation:
Store the PGP Private Key:
Step 1: In the AWS Management Console, navigate to AWS Secrets Manager.
Step 2: Store the PGP private key in Secrets Manager. Ensure the key is encrypted and properly secured.
Set Up the Transfer Family Managed Workflow:
Step 1: In the AWS Transfer Family console, create a new managed workflow.
Step 2: Add a nominal step to the workflow that includes the decryption of the files. Configure this step with the PGP decryption parameters, referencing the PGP private key stored in Secrets Manager.
Step 3: Associate this workflow with the Transfer Family SFTP server, ensuring that incoming files are automatically decrypted upon receipt.
This solution ensures that the data is securely decrypted as it is transferred from the SFTP server to the S3 bucket, automating the decryption process and leveraging AWS Secrets Manager for key management.
Reference
AWS Transfer Family Documentation
Using AWS Secrets Manager for Managing Secrets
AWS Transfer Family Managed Workflows

NEW QUESTION # 453
A company needs to store and process image data that will be uploaded from mobile devices using a custom mobile app. Usage peaks between 8 AM and 5 PM on weekdays, with thousands of uploads per minute. The app is rarely used at any other time A user is notified when image processing is complete.
Which combination of actions should a solutions architect take to ensure image processing can scale to handle the load1? (Select THREE.)

- A. Invoke an AWS Lambda function to perform image processing when a message is available in the queue.
- B. Upload files from the mobile software directly to Amazon S3. Use S3 event notifications to create a message in an Amazon MQ queue.
- C. Send a push notification to the mobile app by using Amazon Simple Notification Service (Amazon SNS) when processing is complete.
- D. Send a push notification to the mobile app by using Amazon Simple Email Service (Amazon SES) when processing is complete.
- E. Upload files from the mobile software directly to Amazon S3. Use S3 event notifications to create a message in an Amazon Simple Queue Service (Amazon SQS) standard queue.
- F. Invoke an S3 Batch Operations job to perform image processing when a message is available in the queue.

Answer: A,C,E

Explanation:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/batch-ops-basics.html

NEW QUESTION # 454
A company runs a popular web application in an on-premises data center. The application receives four million views weekly. The company expects traffic to increase by 200% because of an advertisement that will be published soon.
The company needs to decrease the load on the origin before the increase of traffic occurs. The company does not have enough time to move the entire application to the AWS Cloud.
Which solution will meet these requirements?

- A. Create an accelerator in AWS Global Accelerator. Add listeners for HTTP and HTTPS TCP ports.
  Create an endpoint group. Create a Network Load Balancer (NLB), and attach it to the endpoint group.
  Point the NLB to the on-premises servers. Offload the DNS querying to AWS to handle AWS Global Accelerator traffic.
- B. Create an accelerator in AWS Global Accelerator. Add listeners for HTTP and HTTPS TCP ports.Create an endpoint

group. Create an Application Load Balancer (ALB), and attach it to the endpoint group. Point the ALB to the on-premises servers. Offload the DNS querying to AWS to handle AWS Global Accelerator traffic.

- C. Create an Amazon CloudFront content delivery network (CDN). Enable query forwarding to the origin. Create a managed cache policy that includes query strings. Use an on-premises load balancer as the origin. Offload the DNS querying to AWS to handle CloudFront CDN traffic.
- D. Create an Amazon CloudFront content delivery network (CDN) that uses a Real Time Messaging Protocol (RTMP) distribution. Enable query forwarding to the origin. Use an on-premises load balancer as the origin. Offload the DNS querying to AWS to handle CloudFront CDN traffic.

Answer: B

NEW QUESTION # 455
A company has deployed applications to thousands of Amazon EC2 instances in an AWS account. A security audit discovers that several unencrypted Amazon EBS volumes are attached to the EC2 instances. The company's security policy requires the EBS volumes to be encrypted.
The company needs to implement an automated solution to encrypt the EBS volumes. The solution also must prevent development teams from creating unencrypted EBS volumes.
Which solution will meet these requirements?

- A. Configure the AWS Config managed rule that identifies unencrypted EBS volumes. Configure an automatic remediation action. Associate an AWS Systems Manager Automation runbook that includes the steps to create a new encrypted EBS volume. Create an AWS KMS customer managed key. In the key policy, include a statement to deny the creation of unencrypted EBS volumes.
- B. Use AWS Systems Manager Fleet Manager to create a list of unencrypted EBS volumes. Create a Systems Manager Automation runbook that includes the steps to create a new encrypted EBS volume. Create an SCP to deny the creation of unencrypted EBS volumes.
- C. Configure the AWS Config managed rule that identifies unencrypted EBS volumes. Configure an automatic remediation action. Associate an AWS Systems Manager Automation runbook that includes the steps to create a new encrypted EBS volume. Modify the AWS account setting for EBS encryption to always encrypt new EBS volumes.
- D. Use AWS Systems Manager Fleet Manager to create a list of unencrypted EBS volumes. Create a Systems Manager Automation runbook that includes the steps to create a new encrypted EBS volume. Modify the AWS account setting for EBS encryption to always encrypt new EBS volumes.

Answer: C

NEW QUESTION # 456
A company has several AWS Lambda functions written in Python. The functions are deployed with the .zip package deployment type. The functions use a Lambda layer that contains common libraries and packages in a .zip file. The Lambda .zip packages and the Lambda layer .zip file are stored in an Amazon S3 bucket.
The company must implement automatic scanning of the Lambda functions and the Lambda layer to identify CVEs. A subset of the Lambda functions must receive automated code scans to detect potential data leaks and other vulnerabilities. The code scans must occur only for selected Lambda functions, not all the Lambda functions.
Which combination of actions will meet these requirements? (Select THREE.)

- A. Activate Amazon Inspector. Start automated CVE scans.
- B. Use Amazon Inspector to scan the S3 bucket that contains the Lambda .zip packages and the Lambda layer .zip file for code scans.
- C. Activate Lambda standard scanning and Lambda code scanning in Amazon Inspector.
- D. Enable Amazon GuardDuty. Enable the Lambda Protection feature in GuardDuty.
- E. Enable scanning in the Monitor settings of the Lambda functions that need code scans.
- F. Tag Lambda functions that do not need code scans. In the tag, include a key of InspectorCodeExclusion and a value of LambdaCodeScanning.

Answer: C,E,F

Explanation:
The company requires two different types of security analysis: vulnerability scanning for CVEs and code- level scanning for sensitive data exposure. Amazon Inspector provides both Lambda Standard Scanning and Lambda Code Scanning. These capabilities allow Inspector to examine Lambda deployment packages and Lambda layers for software vulnerabilities, and also perform static code

analysis to detect insecure coding patterns. To meet the requirement that only certain Lambda functions receive deeper code scanning, Inspector allows enabling or disabling code scanning at the individual Lambda function level through the function's Monitor settings. Inspector additionally supports resource exclusion based on tagging, allowing administrators to prevent specific Lambda functions from participating in code scans. Tag-based exclusion satisfies the requirement to scan only a subset of Lambda functions.
Option B is required because enabling both Lambda standard scanning and Lambda code scanning activates the functionality necessary for CVE detection and code security analysis.
Option D is required because enabling scanning at the function level ensures that code scanning runs only for selected Lambda functions.
Option E is required because resource exclusion using tags allows the administrator to exclude non-target Lambda functions from code scanning automatically.
Options A and C do not satisfy the requirement because simply activating Amazon Inspector does not configure per-function scanning behavior, and GuardDuty Lambda Protection does not scan for CVEs or code vulnerabilities. Option F is not valid because Amazon Inspector does not perform scans directly against objects stored in Amazon S3; scanning occurs against the deployed Lambda function versions themselves.

NEW QUESTION # 457
.....