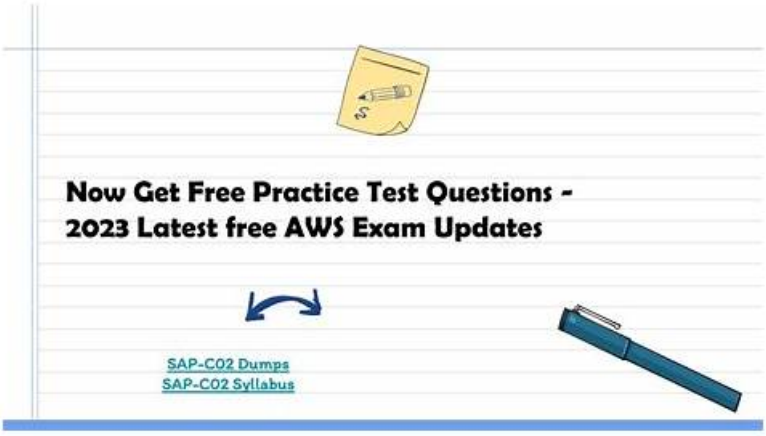
New SAP-C02 Test Prep - Latest SAP-C02 Practice Questions



What's more, part of that TestKingFree SAP-C02 dumps now are free: https://drive.google.com/open?id=1TOrLtfdJqHrvFLK94TMwCjt7iz7YI6kY

In order to be able to better grasp the proposition thesis direction, the AWS Certified Solutions Architect - Professional (SAP-C02) study question focus on proposition which one recent theory and published, in all kinds of academic report even if update to find effective thesis points, according to the proposition of preferences and habits, ponder proposition style of topic selection, to update our SAP-C02 Exam Question, to facilitate users of online learning, better fit time development hot spot.

Passing the Amazon SAP-C02 certification exam is a significant achievement for any cloud computing professional. AWS Certified Solutions Architect - Professional (SAP-C02) certification demonstrates an individual's expertise in AWS architecture and provides a competitive edge in the job market. Additionally, certified professionals can expect to earn higher salaries and be considered for more advanced roles within their organizations. Overall, the Amazon SAP-C02 Certification is a valuable investment for professionals looking to advance their careers in cloud computing.

>> New SAP-C02 Test Prep <<

Latest Amazon SAP-C02 Practice Questions - Cert SAP-C02 Exam

With the SAP-C02 certification you can gain a range of career benefits which include credibility, marketability, validation of skills, and access to new job opportunities. And then you need to enroll in the SAP-C02 exam and prepare well to crack this SAP-C02 Exam with good scores. The TestKingFree will provide you with real, updated, and error-free Amazon SAP-C02 Exam Dumps that will enable you to pass the final SAP-C02 exam easily.

To be eligible for the SAP-C02 certification exam, candidates must have a minimum of two years of experience in designing and deploying AWS-based applications. They should also have experience with multiple AWS services, including VPC, EC2, RDS, S3, and Lambda. Additionally, candidates should also have experience with other AWS services, such as CloudFormation, CloudTrail, CloudWatch, and IAM. The SAP-C02 Certification Exam is a challenging exam that requires a deep understanding of AWS services and a mastery of the skills needed to design and deploy enterprise-level solutions in the AWS cloud. Passing this certification exam can be a significant achievement for professionals who want to advance their career in the field of cloud computing.

Amazon AWS Certified Solutions Architect - Professional (SAP-C02) Sample Questions (Q316-Q321):

NEW QUESTION # 316
A company is building an application that will run on an AWS Lambda function. Hundreds of customers will use the application. The company wants to give each customer a quota of requests for a specific time period.
The quotas must match customer usage patterns. Some customers must receive a higher quota for a shorter time period.
Which solution will meet these requirements?

- A. Create an Amazon API Gateway REST API with a proxy integration to invoke the Lambda function.For each customer, configure an API Gateway usage plan that includes an appropriate request quota.Create an API key from the usage plan for each user that the customer needs.
- B. Create an Amazon API Gateway HTTP API with a proxy integration to invoke the Lambda function.For each customer, configure an API Gateway usage plan that includes an appropriate request quota.Configure route-level throttling for each usage plan. Create an API key from the usage plan for each user that the customer needs.
- C. Create a Lambda function alias for each customer. Include a concurrency limit with an appropriate request quota. Create a Lambda function URL for each function alias. Share the Lambda function URL for each alias with the relevant customer.
- D. Create an Application Load Balancer (ALB) in a VPC. Configure the Lambda function as a target for the ALB. Configure an AWS WAF web ACL for the ALB. For each customer, configure a rate-based rule that includes an appropriate request quota.

Answer: A

Explanation:
Explanation
The correct answer is A.
A: This solution meets the requirements because it allows the company to create different usage plans for each customer, with different request quotas and time periods. The usage plans can be associated with API keys, which can be distributed to the users of each customer. The API Gateway REST API can invoke the Lambda function using a proxy integration, which passes the request data to the function as input and returns the function output as the response. This solution is scalable, secure, and cost-effective12 B: This solution is incorrect because API Gateway HTTP APIs do not support usage plans or API keys. These features are only available for REST APIs3 C: This solution is incorrect because it does not provide a way to enforce request quotas for each customer.
Lambda function aliases can be used to create different versions of the function, but they do not have any quota mechanism. Moreover, this solution exposes the Lambda function URLs directly to the customers, which is not secure or recommended4 D: This solution is incorrect because it does not provide a way to differentiate between customers or users.
AWS WAF rate-based rules can be used to limit requests based on IP addresses, but they do not support any other criteria such as user agents or headers. Moreover, this solution adds unnecessary complexity and cost by using an ALB and a VPC56 References:
1: Creating and using usage plans with API keys - Amazon API Gateway 2: Set up a proxy integration with a Lambda proxy integration - Amazon API Gateway 3: Choose between HTTP APIs and REST APIs - Amazon API Gateway 4: Using AWS Lambda aliases - AWS Lambda 5: Rate-based rule statement - AWS WAF, AWS Firewall Manager, and AWS Shield Advanced 6: Lambda functions as targets for Application Load Balancers
- Elastic Load Balancing

NEW QUESTION # 317
A security engineer determined that an existing application retrieves credentials to an Amazon RDS for MySQL database from an encrypted file in Amazon S3. For the next version of the application, the security engineer wants to implement the following application design changes to improve security:
The database must use strong, randomly generated passwords stored in a secure AWS managed service.
The application resources must be deployed through AWS CloudFormation.
The application must rotate credentials for the database every 90 days.
A solutions architect will generate a CloudFormation template to deploy the application.
Which resources specified in the CloudFormation template will meet the security engineer's requirements with the LEAST amount of operational overhead?

- A. Generate the database password as a secret resource using AWS Secrets Manager. Create an AWS Lambda function resource to rotate the database password. Create an Amazon EventBridge scheduled rule resource to trigger the Lambda function password rotation every 90 days.
- B. Generate the database password as a secret resource using AWS Secrets Manager. Create an AWS Lambda function resource to rotate the database password. Specify a Secrets Manager RotationSchedule resource to rotate the database password every 90 days.
- C. Generate the database password as a SecureString parameter type using AWS Systems Manager Parameter Store. Create an AWS Lambda function resource to rotate the database password. Specify a Parameter Store RotationSchedule resource to rotate the database password every 90 days.
- D. Generate the database password as a SecureString parameter type using AWS Systems Manager Parameter Store. Specify an AWS AppSync DataSource resource to automatically rotate the database password every 90 days.

Answer: C

Explanation:
Explanation
https://aws.amazon.com/blogs/security/how-to-securely-provide-database-credentials-to-lambda-functions-by-us
https://docs.aws.amazon.com/secretsmanager/latest/userguide/rotating-secrets.html
https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating_cloudformation.html

NEW QUESTION # 318
A company has a new requirement to store all database backups in an isolated AWS account. The company is using AWS Organizations and has created a central write-once, read-many (WORM) account for the backups.
The company has 40 Amazon RDS for MySQL databases in its production account. The databases are encrypted with the default RDS AWS KMS key. RDS automated backups of the databases occur daily and have a retention period of 30 days.
Which solution will successfully copy the database backups to the central account?

- A. Create an Amazon EventBridge rule to invoke an AWS Lambda function every day. In the production account, share the default RDS KMS key with the central account. Program the Lambda function to decrypt the snapshots and to initiate a copy request of all unencrypted snapshots to the central account.After the copy job is complete, encrypt the database snapshots with the shared default RDS KMS key in the central account.
- B. Create an Amazon EventBridge rule to invoke an AWS Lambda function every day. Program the Lambda function to decrypt the snapshots and to initiate a copy request of all unencrypted snapshots to the central account. After the copy job is complete, create a new KMS key. Use the new KMS key to encrypt the database snapshots in the central account.
- C. Enable Organizations trusted access and backup policies for AWS Backup. Configure the central account as the delegated administrator for AWS Backup. Create IAM policies and backup policies.
  Enable cross-account management. Create a backup vault in the central account. Create a KMS key for the backup vault and share the key with the production account. In the production account, restore the databases from a snapshot and apply the shared KMS key to the new DB instances. Create a backup plan in the central account to back up the databases to the backup vault.
- D. Enable Organizations trusted access and backup policies for AWS Backup. Configure the central account as the delegated administrator for AWS Backup. Create IAM policies and backup policies.
  Enable cross-account management. In the production account, share the default RDS KMS key with the central account. Create a backup vault in the central account. Apply the shared default RDS KMS key to the backup vault. Create a backup plan in the central account to back up the databases to the backup vault.

Answer: C

Explanation:
The company wants backups to be stored in an isolated central account designed for WORM storage. With AWS Organizations, AWS Backup supports centralized, cross-account backup management through delegated administration, backup policies, and cross-account backup vault usage. This provides the least operational overhead and scales to dozens of databases.
A key constraint is encryption. The databases are encrypted with the default RDS AWS KMS key. AWS- managed KMS keys (including the default RDS KMS key) are not customer-managed and generally cannot be shared across accounts for cross-account snapshot copy and cross-account backup workflows that require key sharing and explicit grants. For cross-account backup copies, the source backups must be encrypted with a customer managed KMS key that can be shared (via key policy and grants) with the destination account.
Therefore, the company must move away from using the default RDS AWS-managed key for encryption of snapshots that will be copied across accounts.
Option A uses the correct managed approach: enable trusted access and backup policies in Organizations, make the central account the delegated administrator, and use AWS Backup to manage cross-account backups into a central backup vault. It also correctly introduces a customer managed KMS key in the central account for the backup vault and shares that key with the production account. Because the existing databases are encrypted with the default RDS AWS-managed key, option A includes the necessary remediation step: restore (or otherwise recreate) the databases so they are encrypted with the shared customer managed KMS key, enabling future backups and copies to be encrypted with a shareable key and stored in the central vault.
Option B is not workable because it requires "sharing the default RDS KMS key" with another account and using it for the central vault. AWS-managed keys are not shared and are not controlled by customers in a way that supports this cross-account backup model. Therefore, this option fails the encryption requirement.
Option C and option D rely on decrypting snapshots, copying them as unencrypted, and then re-encrypting.
This is not a valid or safe operational pattern for RDS automated backups at scale, and it conflicts with typical constraints around snapshot encryption transitions. It also introduces substantial custom automation and operational overhead, and it undermines the objective of a controlled WORM backup account by manipulating encryption state through custom code. Additionally, "decrypting snapshots" is not how encrypted RDS snapshots are typically handled; encrypted snapshots remain encrypted and are copied re-encrypted with a different KMS key that the destination can use, which requires a customer managed key and proper permissions.

Therefore, the successful and scalable solution is to centralize backups with AWS Backup and ensure the databases are encrypted with a customer managed KMS key that can be shared cross-account, as described in option A.
References:
AWS documentation on AWS Backup centralized management with AWS Organizations, including delegated administrator and backup policies for cross-account governance.
AWS documentation on cross-account backup and snapshot copy requirements for encryption, including the need to use AWS KMS customer managed keys for cross-account sharing and re-encryption.
AWS guidance that AWS-managed KMS keys (service-managed default keys) are not shareable across accounts for these cross-account encryption and copy workflows.

NEW QUESTION # 319
A team collects and routes behavioral data for an entire company The company runs a Multi-AZ VPC environment with public subnets, private subnets, and in internet gateway Each public subnet also contains a NAT gateway Most of the company's applications read from and write to Amazon Kinesis Data Streams. Most of the workloads am in private subnets.
A solutions architect must review the infrastructure The solutions architect needs to reduce costs and maintain the function of the applications The solutions architect uses Cost Explorer and notices that the cost in the EC2-Other category is consistently high A further review shows that NatGateway-Bytes charges are increasing the cost in the EC2-Other category.
What should the solutions architect do to meet these requirements?

- A. Enable VPC Flow Logs and Amazon Detective Review Detective findings for traffic that is not related to Kinesis Data Streams Configure security groups to block that traffic
- B. Add an interface VPC endpoint for Kinesis Data Streams to the VPC. Ensure that applications have the correct IAM permissions to use the interface VPC endpoint.
- C. Enable VPC Flow Logs. Use Amazon Athena to analyze the logs for traffic that can be removed. Ensure that security groups are Mocking traffic that is responsible for high costs.
- D. Add an interface VPC endpoint for Kinesis Data Streams to the VPC. Ensure that the VPC endpoint policy allows traffic from the applications.

Answer: D

Explanation:
Explanation
https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-access.html
https://aws.amazon.com/premiumsupport/knowledge-center/vpc-reduce-nat-gateway-transfer-costs/ VPC endpoint policies enable you to control access by either attaching a policy to a VPC endpoint or by using additional fields in a policy that is attached to an IAM user, group, or role to restrict access to only occur via the specified VPC endpoint

NEW QUESTION # 320
A company that develops consumer electronics with offices in Europe and Asia has 60 TB of software images stored on premises in Europe.
The company wants to transfer the images to an Amazon S3 bucket in the ap-northeast-1 Region.
New software images are created daily and must be encrypted in transit.
The company needs a solution that does not require custom development to automatically transfer all existing and new software images to Amazon S3.
What is the next step in the transfer process?

- A. Deploy an AWS DataSync agent and configure a task to transfer the images to the S3 bucket
- B. Configure Amazon Kinesis Data Firehose to transfer the images using S3 Transfer Acceleration
- C. Transfer the images over a Site-to-Site VPN connection using the S3 API with multipart upload
- D. Use an AWS Snowball device to transfer the images with the S3 bucket as the target

Answer: A

Explanation:
DataSync provides built-in security capabilities such as encryption of data in-transit, and data integrity verification in-transit and at-rest. It optimizes use of network bandwidth, and automatically recovers from network connectivity failures. In addition, DataSync provides control and monitoring capabilities such as data transfer scheduling and granular visibility into the transfer process through Amazon CloudWatch metrics, logs, and events.

NEW QUESTION # 321

......

Latest SAP-C02 Practice Questions: https://www.testkingfree.com/Amazon/SAP-C02-practice-exam-dumps.html

P.S. Free 2026 Amazon SAP-C02 dumps are available on Google Drive shared by TestKingFree: https://drive.google.com/open?id=1TOrLtfdJqHrvFLK94TMwCjt7iz7YI6kY