# Pass Guaranteed Quiz Reliable Amazon - Latest SAA-C03 Test Vce

To let the clients be familiar with the atmosphere and pace of the real SAA-C03 exam we provide the function of stimulating the exam. In such a way, our candidates will become more confident by practising on it. And our expert team updates the SAA-C03 Study Guide frequently to let the clients practice more. So the quality of our SAA-C03 practice materials is very high and we can guarantee to you that you will have few difficulties to pass the exam.

To become certified, candidates must pass the SAA-C03 Exam, which consists of 65 multiple-choice and multiple-response questions that must be completed within 130 minutes. SAA-C03 exam is computer-based and can be taken at a testing center or remotely. The passing score for the exam is 720 out of 1000.

Earning the Amazon SAA-C03 Certification provides IT professionals with a competitive edge in the job market and validates their skills in designing and deploying reliable and scalable solutions on the AWS platform. AWS Certified Solutions Architect - Associate certification is recognized globally and is highly sought-after by organizations looking for skilled professionals to manage their AWS infrastructure.

**>> Latest SAA-C03 Test Vce <<**

## Latest Latest SAA-C03 Test Vce – 100% Valid AWS Certified Solutions Architect - Associate Test Engine Version

The AWS Certified Solutions Architect - Associate (SAA-C03) actual questions we sell also come with a free demo. Spend no time, otherwise, you will pass on these fantastic opportunities. Start preparing for the AWS Certified Solutions Architect - Associate (SAA-C03) exam by purchasing the most recent Amazon SAA-C03 exam dumps. You must improve your skills and knowledge to stay current and competitive. You merely need to obtain the SAA-C03 Certification Exam badge in order to achieve this. You must pass the AWS Certified Solutions Architect - Associate SAA-C03 exam to accomplish this, which can only be done with thorough exam preparation. Download the AWS Certified Solutions Architect - Associate (SAA-C03) exam questions right away for immediate and thorough exam preparation.

Amazon SAA-C03 Exam is a valuable certification for IT professionals who want to work with AWS cloud services. AWS Certified Solutions Architect - Associate certification validates the skills and knowledge required to design, deploy, and manage scalable, highly available, and fault-tolerant systems on the AWS platform. It is an essential certification for individuals who want to advance their careers in cloud computing and work for companies that use AWS services. AWS Certified Solutions Architect - Associate certification is also an excellent way for IT professionals to demonstrate their expertise and stand out in a competitive job market.

# Amazon AWS Certified Solutions Architect - Associate Sample Questions (Q84-Q89):

### NEW QUESTION # 84
A company must migrate 20 TB of data from a data center to the AWS Cloud within 30 days. The company's network bandwidth is limited to 15 Mbps and cannot exceed 70% utilization. What should a solutions architect do to meet these requirements?

- A. Use AWS Snowball.
- B. Use Amazon S3 Transfer Acceleration.
- C. Use AWS DataSync.
- D. Use a secure VPN connection.

**Answer: A**

Explanation:
Explanation
AWS Snowball is a secure data transport solution that accelerates moving large amounts of data into and out of the AWS cloud. It can move up to 80 TB of data at a time, and provides a network bandwidth of up to 50 Mbps, so it is well-suited for the task. Additionally, it is secure and easy to use, making it the ideal solution for this migration.

### NEW QUESTION # 85
A company has registered its domain name with Amazon Route 53. The company uses Amazon API Gateway in the ca-central-1 Region as a public interface for its backend microservice APIs. Third-party services consume the APIs securely. The company wants to design its API Gateway URL with the company's domain name and corresponding certificate so that the third-party services can use HTTPS.
Which solution will meet these requirements?

- A. Create a Regional API Gateway endpoint. Associate the API Gateway endpoint with the company's domain name. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us-east-1 Region. Attach the certificate to the API Gateway APIs.Create Route 53 DNS records with the company's domain name. Point an A record to the company's domain name.
- B. Create a Regional API Gateway endpoint. Associate the API Gateway endpoint with the company's domain name. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the same Region. Attach the certificate to the API Gateway endpoint.
Configure Route 53 to route traffic to the API Gateway endpoint.
- C. Create stage variables in API Gateway with Name="Endpoint-URL" and Value="Company Domain Name" to overwrite the default URL. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM).
- D. Create Route 53 DNS records with the company's domain name. Point the alias record to the Regional API Gateway stage endpoint. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us-east-1 Region.

**Answer: B**

Explanation:

Explanation
To design the API Gateway URL with the company's domain name and corresponding certificate, the company needs to do the following: 1. Create a Regional API Gateway endpoint: This will allow the company to create an endpoint that is specific to a region. 2. Associate the API Gateway endpoint with the company's domain name: This will allow the company to use its own domain name for the API Gateway URL. 3. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the same Region: This will allow the company to use HTTPS for secure communication with its APIs. 4. Attach the certificate to the API Gateway endpoint: This will allow the company to use the certificate for securing the API Gateway URL. 5. Configure Route 53 to route traffic to the API Gateway endpoint: This will allow the company to use Route 53 to route traffic to the API Gateway URL using the company's domain name.

**NEW QUESTION # 86**
A company runs multiple workloads on virtual machines (VMs) in an on-premises data center. The company is expanding rapidly. The on-premises data center is not able to scale fast enough to meet business needs. The company wants to migrate the workloads to AWS.
The migration is time sensitive. The company wants to use a lift-and-shift strategy for non-critical workloads.
Which combination of steps will meet these requirements? (Select THREE.)

- A. Use AWS App2Container (A2C) to collect data about the VMs.
- B. Stop all operations on the VMs Launch a cutover instance.
- C. Use the AWS Schema Conversion Tool (AWS SCT) to collect data about the VMs.
- D. Use AWS Database Migration Service (AWS DMS) to migrate the VMs.
- E. Use AWS Application Migration Service. Install the AWS Replication Agent on the VMs.
- F. Complete the initial replication of the VMs. Launch test instances to perform acceptance tests on the VMs.

**Answer: B,E,F**

Explanation:
AWS Application Migration Service (AWS MGN) is the recommended tool for a lift-and-shift strategy, especially for time-sensitive migrations. It automates the replication of on-premises VMs to AWS, minimizing the effort required for migration and testing.
Key steps:
* Replication with AWS MGN: The AWS Replication Agent is installed on the VMs to continuously replicate data to AWS, allowing you to manage migration easily.
* Testing and Cutover: Initial replication allows for testing in AWS before performing the final cutover, ensuring that the migration process is smooth and data integrity is maintained.
* AWS Documentation: AWS MGN is recommended for migrating virtual machines to the cloud with minimal downtime and disruption.

**NEW QUESTION # 87**
A media company is launching a new product platform that artists from around the world can use to upload videos and images directly to an Amazon S3 bucket. The company owns and maintains the S3 bucket. The artists must be able to upload files from personal devices without the need for AWS credentials or an AWS account.
Which solution will meet these requirements MOST securely?

- A. Create a web interface that uses an IAM role that has permission to upload and view objects in the S3 bucket. Share the web interface URL to the artists.
- B. Use an IAM role that has upload permissions for the S3 bucket to generate presigned URLs for S3 prefixes that are specific to each artist. Share the URLs to the artists.
- C. Turn off block public access for the S3 bucket. Share the bucket URL to the artists to enable uploads without credentials.
- D. Enable cross-origin resource sharing (CORS) on the S3 bucket.

**Answer: B**

Explanation:
Option C is the most secure and practical solution. Presigned URLs allow temporary, limited access to upload files to specific S3 prefixes. This ensures that artists can upload files securely without needing AWS credentials or accounts. Each artist receives a unique URL with permissions tied to the intended S3 location, and the URL can be configured to expire after a certain time, minimizing security risks.
Why Other Options Are Incorrect:
* Option A: Enabling CORS allows cross-origin access but does not provide authentication or authorization for uploads. This does

not secure the uploads or restrict access to specific artists.
* Option B: Turning off block public access and sharing the bucket URL exposes the bucket to potential misuse and unauthorized uploads. This approach is highly insecure.
* Option D: While a web interface might work, it introduces additional complexity and potential security risks by exposing upload functionality through a public-facing application.
AWS Documentation References:
* Using Amazon S3 Presigned URLs
* AWS Best Practices for Secure S3 Access

## NEW QUESTION # 88
[Design Secure Architectures]
A company is building an Amazon Elastic Kubernetes Service (Amazon EKS) cluster for its workloads. All secrets that are stored in Amazon EKS must be encrypted in the Kubernetes etcd key-value store.
Which solution will meet these requirements?

- A. Create a new AWS Key Management Service (AWS KMS) key with the ahas/aws/ebs alias Enable default Amazon Elastic Block Store (Amazon EBS) volume encryption for the account.
- B. Create the Amazon EKS cluster with default options Use the Amazon Elastic Block Store (Amazon EBS) Container Storage Interface (CSI) driver as an add-on.
- C. Create a new AWS Key Management Service (AWS KMS) key Use AWS Secrets Manager to manage rotate, and store all secrets in Amazon EKS.
- D. Create a new AWS Key Management Service (AWS KMS) key Enable Amazon EKS KMS secrets encryption on the Amazon EKS cluster.

**Answer: D**

Explanation:
This option is the most secure and simple way to encrypt the secrets that are stored in Amazon EKS. AWS Key Management Service (AWS KMS) is a service that allows you to create and manage encryption keys that can be used to encrypt your data. Amazon EKS KMS secrets encryption is a feature that enables you to use a KMS key to encrypt the secrets that are stored in the Kubernetes etcd key-value store. This provides an additional layer of protection for your sensitive data, such as passwords, tokens, and keys. You can create a new KMS key or use an existing one, and then enable the Amazon EKS KMS secrets encryption on the Amazon EKS cluster. You can also use IAM policies to control who can access or use the KMS key.
Option A is not correct because using AWS Secrets Manager to manage, rotate, and store all secrets in Amazon EKS is not necessary or efficient. AWS Secrets Manager is a service that helps you securely store, retrieve, and rotate your secrets, such as database credentials, API keys, and passwords. You can use it to manage secrets that are used by your applications or servicesoutside of Amazon EKS, but it is not designed to encrypt the secrets that are stored in the Kubernetes etcd key-value store. Moreover, using AWS Secrets Manager would incur additional costs and complexity, and it would not leverage the native Kubernetes secrets management capabilities.
Option C is not correct because using the Amazon EBS Container Storage Interface (CSI) driver as an add-on does not encrypt the secrets that are stored in Amazon EKS. The Amazon EBS CSI driver is a plugin that allows you to use Amazon EBS volumes as persistent storage for your Kubernetes pods. It is useful for providing durable and scalable storage for your applications, but it does not affect the encryption of the secrets that are stored in the Kubernetes etcd key-value store. Moreover, using the Amazon EBS CSI driver would require additional configuration and resources, and it would not provide the same level of security as using a KMS key.
Option D is not correct because creating a new AWS KMS key with the alias aws/ebs and enabling default Amazon EBS volume encryption for the account does not encrypt the secrets that are stored in Amazon EKS. The alias aws/ebs is a reserved alias that is used by AWS to create a default KMS key for your account. This key is used to encrypt the Amazon EBS volumes that are created in your account, unless you specify a different KMS key. Enabling default Amazon EBS volume encryption for the account is a setting that ensures that all new Amazon EBS volumes are encrypted by default. However, these features do not affect the encryption of the secrets that are stored in the Kubernetes etcd key-value store. Moreover, using the default KMS key or the default encryption setting would not provide the same level of control and security as using a custom KMS key and enabling the Amazon EKS KMS secrets encryption feature. Reference:
Encrypting secrets used in Amazon EKS
What Is AWS Key Management Service?
What Is AWS Secrets Manager?
Amazon EBS CSI driver
Encryption at rest

**NEW QUESTION # 89**

......

**SAA-C03 Test Engine Version**: https://www.briandumpsprep.com/SAA-C03-prep-exam-braindumps.html