Also check out this article: **Top 5 FREE AWS Review Materials**.

# Common Exam Scenarios for the SAA-C03 exam

| Scenario | Solution |
|---|---|
| **Domain 1: Design Resilient Architectures** | |
| Set up asynchronous data replication to another RDS DB instance hosted in another AWS Region | Create a Read Replica |
| A parallel file system for "hot" (frequently accessed) data | Amazon FSx For Lustre |
| Implement synchronous data replication across Availability Zones with automatic failover in Amazon RDS. | Enable Multi-AZ deployment in Amazon RDS. |
| Needs a storage service to host "cold" (infrequently accessed) data | Amazon S3 Glacier |
| Set up a relational database and a disaster recovery plan with an RPO of 1 second and RTO of less than 1 minute. | Use Amazon Aurora Global Database. |
| Monitor database metrics and send email notifications if a specific threshold has been breached. | Create an SNS topic and add the topic in the CloudWatch alarm. |
| Set up a DNS failover to a static website. | Use Route 53 with the failover option to a static S3 website bucket or CloudFront distribution. |
| Implement an automated backup for all the EBS Volumes. | Use Amazon Data Lifecycle Manager to automate the creation of EBS snapshots. |
| Monitor the available swap space of your EC2 instances | Install the CloudWatch agent and monitor the SwapUtilizationmetric. |

| | |
|---|---|
| Implement a 90-day backup retention policy on **Amazon Aurora**. | Use **AWS Backup** |

| Domain 2: Design High-Performing Architectures | |
|---|---|
| Implement a fanout messaging. | Create an SNS topic with a message filtering policy and configure multiple SQS queues to subscribe to the topic. |
| A database that has a read replication latency of less than 1 second. | Use Amazon Aurora with cross-region replicas. |
| A specific type of Elastic Load Balancer that uses UDP as the protocol for communication between clients and thousands of game servers around the world. | Use Network Load Balancer for TCP/UDP protocols. |
| Monitor the memory and disk space utilization of an EC2 instance. | Install Amazon CloudWatch agent on the instance. |
| Retrieve a subset of data from a large CSV file stored in the S3 bucket. | Perform an S3 Select operation based on the bucket's name and object's key. |
| Upload 1 TB file to an S3 bucket. | Use Amazon S3 multipart upload API to upload large objects in parts. |
| Improve the performance of the application by reducing the response times from milliseconds to microseconds. | Use **Amazon DynamoDB** Accelerator (DAX) |
| Retrieve the instance ID, public keys, and public IP address of an EC2 instance. | Access the URL: http://169.254.169.254/latest/meta-data/ using the EC2 instance. |
| Route the internet traffic to the resources based on the location of the user. | Use Route 53 Geolocation Routing policy. |
| A fully managed ETL (extract, transform, and load) service provided by Amazon Web Services. | AWS Glue |
| A fully managed, petabyte-scale data warehouse | Amazon Redshift |

| | |
|---|---|
| service. | |

| Domain 3: Design Secure Applications and Architectures | |
|---|---|
| Encrypt EBS volumes restored from the unencrypted EBS snapshots | Copy the snapshot and enable encryption with a new symmetric CMK while creating an EBS volume using the snapshot. |
| Limit the maximum number of requests from a single IP address. | Create a rate-based rule in AWS WAF and set the rate limit. |
| Grant the bucket owner full access to all uploaded objects in the S3 bucket. | Create a bucket policy that requires users to set the object's ACL to bucket-owner-full-control. |
| Protect objects in the S3 bucket from accidental deletion or overwrite. | Enable versioning and MFA delete. |
| Access resources on both on-premises and AWS using on-premises credentials that are stored in Active Directory. | Set up SAML 2.0-Based Federation by using a Microsoft Active Directory Federation Service. |
| Secure the sensitive data stored in EBS volumes | Enable EBS Encryption |
| Ensure that the data-in-transit and data-at-rest of the Amazon S3 bucket is always encrypted | Enable Amazon S3 Server-Side or use Client-Side Encryption |
| Secure the web application by allowing multiple domains to serve SSL traffic over the same IP address. | Use AWS Certificate Manager to generate an SSL certificate. Associate the certificate to the CloudFront distribution and enable Server Name Indication (SNI). |
| Control the access for several S3 buckets by using a gateway endpoint to allow access to trusted buckets. | Create an endpoint policy for trusted S3 buckets. |
| Enforce strict compliance by tracking all the configuration changes made to any AWS services. | Set up a rule in AWS Config to identify compliant and non-compliant services. |
| Provide short-lived access tokens that act as temporary security credentials to allow access to AWS resources. | Use AWS Security Token Service |

| | |
|---|---|
| Encrypt and rotate all the database credentials, API keys, and other secrets on a regular basis. | Use AWS Secrets Manager and enable automatic rotation of credentials. |

| **Domain 4: Design Cost-Optimized Architectures** | |
|---|---|
| A cost-effective solution for over-provisioning of resources. | Configure a target tracking scaling in ASG. |
| The application data is stored in a tape backup solution. The backup data must be preserved for up to 10 years. | Use AWS Storage Gateway to backup the data directly to Amazon S3 Glacier Deep Archive. |
| Accelerate the transfer of historical records from on-premises to AWS over the Internet in a cost-effective manner. | Use AWS DataSync and select Amazon S3 Glacier Deep Archive as the destination. |
| Globally deliver the static contents and media files to customers around the world with low latency. | Store the files in Amazon S3 and create a CloudFront distribution. Select the S3 bucket as the origin. |
| An application must be hosted to two EC2 instances and should continuously run for three years. The CPU utilization of the EC2 instances is expected to be stable and predictable. | Deploy the application to a Reserved instance. |
| Implement a cost-effective solution for S3 objects that are accessed less frequently. | Create an Amazon S3 lifecyle policy to move the objects to Amazon S3 Standard-IA. |
| Minimize the data transfer costs between two EC2 instances. | Deploy the EC2 instances in the same Region. |
| Import the SSL/TLS certificate of the application. | Import the certificate into AWS Certificate Manager or upload it to AWS IAM. |

# AWS Certified Solutions Architect Associate Video Course – SAA-C03