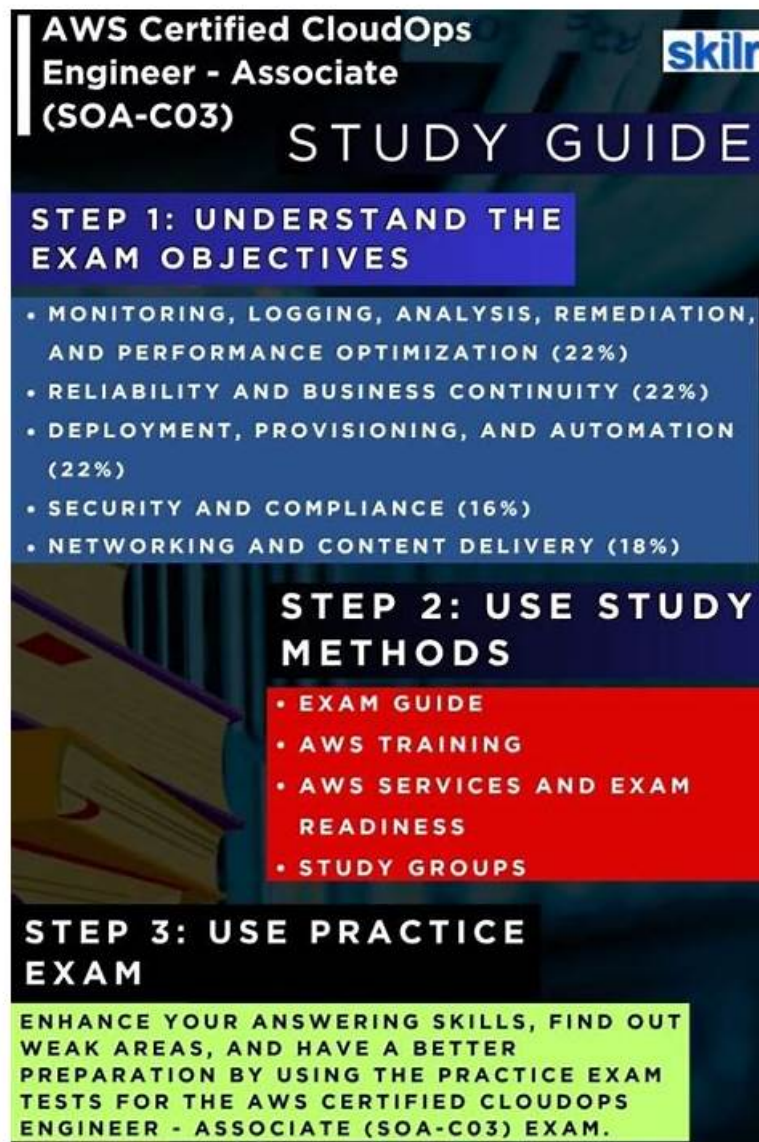


SOA-C03 Study Plan & SOA-C03 PDF Question



P.S. Free 2026 Amazon SOA-C03 dumps are available on Google Drive shared by Dumpexams: <https://drive.google.com/open?id=1ohgfkG8mOK-VQ8FPekVPbkw67Kr0TuT3>

We provide free update to the clients within one year. The clients can get more SOA-C03 study materials to learn and understand the latest industry trend. We boost the specialized expert team to take charge for the update of SOA-C03 study materials timely and periodically. They refer to the excellent published authors' thesis and the latest emerging knowledge points among the industry to update our SOA-C03 Study Materials. After one year, the clients can enjoy 50 percent discounts and the old clients enjoy some certain discounts when purchasing. So the clients can enjoy more benefits after they buy our SOA-C03 study materials.

Amazon SOA-C03 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">• Security and Compliance: This section measures skills of Security Engineers and includes implementing IAM policies, roles, MFA, and access controls. It focuses on troubleshooting access issues, enforcing compliance, securing data at rest and in transit using AWS KMS and ACM, protecting secrets, and applying findings from Security Hub, GuardDuty, and Inspector.

Topic 2	<ul style="list-style-type: none"> • Networking and Content Delivery: This section measures skills of Cloud Network Engineers and focuses on VPC configuration, subnets, routing, network ACLs, and gateways. It includes optimizing network cost and performance, configuring DNS with Route 53, using CloudFront and Global Accelerator for content delivery, and troubleshooting network and hybrid connectivity using logs and monitoring tools.
Topic 3	<ul style="list-style-type: none"> • Monitoring, Logging, Analysis, Remediation, and Performance Optimization: This section of the exam measures skills of CloudOps Engineers and covers implementing AWS monitoring tools such as CloudWatch, CloudTrail, and Prometheus. It evaluates configuring alarms, dashboards, and notifications, analyzing performance metrics, troubleshooting issues using EventBridge and Systems Manager, and applying strategies to optimize compute, storage, and database performance.
Topic 4	<ul style="list-style-type: none"> • Reliability and Business Continuity: This section measures the skills of System Administrators and focuses on maintaining scalability, elasticity, and fault tolerance. It includes configuring load balancing, auto scaling, Multi-AZ deployments, implementing backup and restore strategies with AWS Backup and versioning, and ensuring disaster recovery to meet RTO and RPO goals.
Topic 5	<ul style="list-style-type: none"> • Deployment, Provisioning, and Automation: This section measures the skills of Cloud Engineers and covers provisioning and maintaining cloud resources using AWS CloudFormation, CDK, and third-party tools. It evaluates automation of deployments, remediation of resource issues, and managing infrastructure using Systems Manager and event-driven processes like Lambda or S3 notifications.

>> SOA-C03 Study Plan <<

Diverse Formats for Amazon SOA-C03 Exam Questions: Choose What Works Best for You

Through years of efforts and constant improvement, our SOA-C03 exam materials stand out from numerous study materials and become the top brand in the domestic and international market. Our company controls all the links of SOA-C03 training materials which include the research, innovation, survey, production, sales and after-sale service strictly and strives to make every link reach the acme of perfection. Our company pays close attentions to the latest tendency among the industry and the clients' feedback about our SOA-C03 Certification guide.

Amazon AWS Certified CloudOps Engineer - Associate Sample Questions (Q14-Q19):

NEW QUESTION # 14

A CloudOps engineer needs to build an event infrastructure for custom application-specific events. The events must be sent to an AWS Lambda function for processing. The CloudOps engineer must record the events so they can be replayed later by event type or event time.

Which solution will meet these requirements?

- **A. Create an Amazon EventBridge custom event bus, create an archive, and create a rule to send events to Lambda.**
- B. Create an archive on the default event bus and use pattern matching.
- C. Create an EventBridge pipe and store events in an archive.
- D. Create a CloudWatch Logs log group and route events there.

Answer: A

Explanation:

Comprehensive Explanation (250-350 words):

Amazon EventBridge supports custom event buses for application-specific events. EventBridge archives allow events to be retained and replayed later based on time ranges or event patterns, directly meeting the replay requirement.

Creating a custom event bus provides isolation and governance for application events. The archive preserves events automatically, and EventBridge rules route events to AWS Lambda for processing without custom code.

Options B and C do not properly align with custom event use cases or supported archive behavior. Option D lacks native replay functionality.

Therefore, a custom event bus with an archive and rule is the correct solution.

NEW QUESTION # 15

A company needs to log and audit any principal that publishes messages to Amazon Simple Notification Service (Amazon SNS) topics and Amazon Simple Queue Service (Amazon SQS) queues. The company wants to ensure that all communication with these services uses VPC endpoints.

Which combination of solutions will meet these requirements? (Select TWO.)

- A. Set up AWS CloudTrail. Enable tracking of data events for Amazon SNS and Amazon SQS. Deliver logs to an Amazon S3 bucket for querying.
- B. Configure VPC endpoints for Amazon SNS and Amazon SQS. Inspect the `vpcEndpoint` field in the Amazon CloudWatch logs.
- C. Create Amazon EventBridge rules to gather Amazon SNS and Amazon SQS events. Store the events in an Amazon S3 bucket.
- D. Use Amazon CloudWatch Logs to collect message content from Amazon SNS and Amazon SQS. Deliver logs to an Amazon S3 bucket for querying.
- E. Configure VPC endpoints for Amazon SNS and Amazon SQS. Inspect the `vpcEndpointId` field in the AWS CloudTrail logs.

Answer: A,E

Explanation:

Comprehensive and Detailed Explanation From Exact Extract of AWS CloudOps Documents:

To meet the requirement to log and audit any principal that publishes to SNS topics and interacts with SQS queues, the correct service is AWS CloudTrail, because CloudTrail records API activity (who did what, when, and from where). Enabling data events (where supported/required for deeper visibility) provides detailed records for operations such as publishing messages and sending/receiving messages. Delivering CloudTrail logs to Amazon S3 provides durable retention and supports querying workflows. To ensure that communication uses VPC endpoints, the company should configure VPC endpoints for SNS and SQS and then validate usage by inspecting CloudTrail event records. CloudTrail includes endpoint- related context fields (for example, a VPC endpoint identifier) that allow auditors to confirm that the request path used a VPC endpoint rather than traversing the public internet. This directly addresses the "must use VPC endpoints" control with auditable evidence.

The other options do not satisfy both requirements. CloudWatch Logs does not automatically capture SNS /SQS API caller identity for publish/send/receive operations in the same authoritative way CloudTrail does.

EventBridge can capture service events but is not the primary audit log of API calls and does not inherently prove VPC endpoint usage per request. Inspecting a VPC endpoint field in CloudWatch Logs is not the standard audit mechanism for these API calls.

References:

AWS CloudTrail User Guide - Event records, management events, data events, delivery to Amazon S3 Amazon SNS Developer Guide - API actions and logging/auditing considerations Amazon SQS Developer Guide - API actions and logging/auditing considerations Amazon VPC User Guide - Interface VPC endpoints (AWS PrivateLink) and private access to AWS services

NEW QUESTION # 16

A company operates compute resources in a VPC and in the company's on-premises data center. The company already has an AWS Direct Connect connection between the VPC and the on-premises data center. A CloudOps engineer needs to ensure that Amazon EC2 instances in the VPC can resolve DNS names for hosts in the on-premises data center.

Which solution will meet this requirement with the LEAST amount of ongoing maintenance?

- A. Set up a forwarding rule for reverse DNS queries in Amazon Route 53 Resolver. Set the `enableDnsHostnames` attribute to true for the VPC.
- B. Create an Amazon Route 53 private hosted zone. Populate the zone with the hostnames and IP addresses of the hosts in the on-premises data center.
- C. Create an Amazon Route 53 Resolver outbound endpoint. Add the IP addresses of an on- premises DNS server for the domain names that need to be forwarded.
- D. Add the hostnames and IP addresses for the on-premises hosts to the `/etc/hosts` file of each EC2 instance.

Answer: C

Explanation:

The Route 53 Resolver outbound endpoint enables DNS queries from resources in a VPC to be forwarded to on-premises DNS servers over an existing AWS Direct Connect or VPN connection.

By creating forwarding rules that specify which domains should be resolved through the on- premises DNS servers, EC2 instances in the VPC can seamlessly resolve internal hostnames without manual configuration or ongoing maintenance. This is the most scalable

and low- maintenance solution.

NEW QUESTION # 17

A company's website runs on an Amazon EC2 Linux instance. The website needs to serve PDF files from an Amazon S3 bucket. All public access to the S3 bucket is blocked at the account level. The company needs to allow website users to download the PDF files.

Which solution will meet these requirements with the LEAST administrative effort?

- A. Deploy an EC2 instance that has an IAM instance profile to a public subnet. Use a signed URL from the EC2 instance to provide temporary access to the S3 bucket for website users.
- B. Change the S3 bucket permissions to allow public access on the source S3 bucket. Assign a company employee to provide a PDF file URL to users when users request the PDF files.
- C. Create an IAM role that has a policy that allows s3:list* and s3:get* permissions. Assign the role to the EC2 instance. Assign a company employee to download requested PDF files to the EC2 instance and deliver the files to website users. Create an AWS Lambda function to periodically delete local files.
- **D. Create an Amazon CloudFront distribution that uses an origin access control (OAC) that points to the S3 bucket. Apply a bucket policy to the bucket to allow connections from the CloudFront distribution. Assign a company employee to provide a download URL that contains the distribution URL and the object path to users when users request PDF files.**

Answer: D

Explanation:

Per the AWS Cloud Operations, Networking, and Security documentation, the best practice for serving private S3 content securely to end users is to use Amazon CloudFront with Origin Access Control (OAC).

OAC enables CloudFront to access S3 buckets privately, even when Block Public Access settings are enabled at the account level. This allows content to be delivered globally and securely without making the S3 bucket public. The bucket policy explicitly allows access only from the CloudFront distribution, ensuring that users can retrieve PDF files only via CloudFront URLs.

This configuration offers:

Automatic scalability through CloudFront caching,

Improved security via private access control,

Minimal administration effort with fully managed services.

Other options require manual handling or make the bucket public, violating AWS security best practices.

Therefore, Option B-using CloudFront with Origin Access Control and a restrictive bucket policy-provides the most secure, efficient, and low-maintenance CloudOps solution.

NEW QUESTION # 18

A global gaming company is preparing to launch a new game on AWS. The game runs in multiple AWS Regions on a fleet of Amazon EC2 instances. The instances are in an Auto Scaling group behind an Application Load Balancer (ALB) in each Region. The company plans to use Amazon Route 53 for DNS services. The DNS configuration must direct users to the Region that is closest to them and must provide automated failover.

Which combination of steps should a CloudOps engineer take to configure Route 53 to meet these requirements? (Select TWO.)

- **A. Configure Route 53 geoproximity routing. Specify the Regions that are used for the infrastructure.**
- B. Create Amazon CloudWatch alarms that monitor the health of the EC2 instances in each Region. Configure Route 53 DNS failover by using a health check that monitors the alarms.
- C. Configure Route 53 DNS failover by using a health check that monitors the private IP address of an EC2 instance in each Region.
- **D. Create Amazon CloudWatch alarms that monitor the health of the ALB in each Region. Configure Route 53 DNS failover by using a health check that monitors the alarms.**
- E. Configure Route 53 simple routing. Specify the continent, country, and state or province that are used for the infrastructure.

Answer: A,D

Explanation:

The combination of geoproximity routing and DNS failover health checks provides global low-latency routing with high availability. Geoproximity routing in Route 53 routes users to the AWS Region closest to their geographic location, optimizing latency. For automatic failover, Route 53 health checks can monitor CloudWatch alarms tied to the health of the ALB in each Region. When a Region becomes unhealthy, Route 53 reroutes traffic to the next available Region automatically.

AWS documentation states:

References (AWS CloudOps Documents / Study Guide):

- ### NEW QUESTION # 19

• • • • •

SOA-C03 PDF Question: <https://www.dumpexams.com/SOA-C03-real-answers.html>

- P.S. Free & New SOA-C03 dumps are available on Google Drive shared by Dumpexams: <https://drive.google.com/open?id=1ohgfkG8mOK-VO8FPekVPbkw67Kr0TuT3>