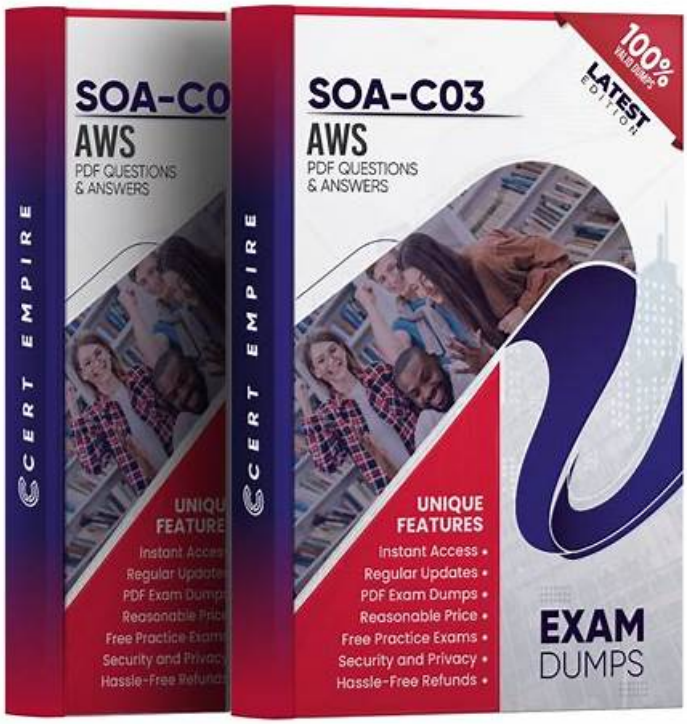
New SOA-C03 Test Camp - SOA-C03 Exam Fee



DOWNLOAD the newest PassReview SOA-C03 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=134fZvBEj4jaE8CXMpdJ2wBgp8RUGN4Z2

For some difficult points of the SOA-C03 exam questions which you may feel hard to understand or easy to confuse for too similar with the others. In order to help you memorize the SOA-C03 guide materials better, we have detailed explanations of the difficult questions such as illustration, charts and referring website. Every year some knowledge of the SOA-C03 Practice Braindumps is reoccurring over and over. You must ensure that you master them completely.

Our products are officially certified, and our SOA-C03 exam materials are definitely the most authoritative product in the industry. In order to ensure the authority of our SOA-C03 practice prep, our company has really taken many measures. We have hired the most professioal experts to compile the content of the SOA-C03 study braindumps, and design the displays. So our SOA-C03 learning questions can stand the test of the market.

>> New SOA-C03 Test Camp <<

100% Pass Amazon - High Hit-Rate New SOA-C03 Test Camp

Passing the SOA-C03 Exam is a challenging task, but with PassReview Amazon Practice Test engine, you can prepare yourself for success in one go. The SOA-C03 online practice test engine offers an interactive learning experience and includes Amazon SOA-C03 Practice Questions in a real SOA-C03 Exam scenario. This allows you to become familiar with the SOA-C03 exam format and identify your weak areas to improve them.

Amazon SOA-C03 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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	• 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 3	• 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 4	• 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	• 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.

Amazon AWS Certified CloudOps Engineer - Associate Sample Questions (Q74-Q79):

NEW QUESTION # 74
A company's AWS accounts are in an organization in AWS Organizations. The organization has all features enabled. The accounts use Amazon EC2 instances to host applications. The company manages the EC2 instances manually by using the AWS Management Console. The company applies updates to the EC2 instances by using an SSH connection to each EC2 instance.
The company needs a solution that uses AWS Systems Manager to manage all the organization's current and future EC2 instances. The latest version of Systems Manager Agent (SSM Agent) is running on the EC2 instances.
Which solution will meet these requirements?

- A. Configure a home AWS Region in Systems Manager Quick Setup in the organization's management account. Create a Systems Manager Run Command that attaches the AmazonSSMServiceRolePolicy IAM policy to every IAM role that the EC2 instances use. Invoke the command in every account in the organization.
- B. Configure a home AWS Region in Systems Manager Quick Setup in the organization's management account. Deploy the Systems Manager Default Host Management Configuration Quick Setup from the management account.
- C. Create an AWS CloudFormation stack set that contains a Systems Manager parameter to define the Default Host Management Configuration role. Use the organization's management account to deploy the stack set to every account in the organization.
- D. Create an AWS CloudFormation stack set that contains an EC2 instance profile with the AmazonSSMManagedEC2InstanceDefaultPolicy IAM policy attached. Use the organization's management account to deploy the stack set to every account in the organization.

Answer: B

Explanation:
AWS CloudOps automation best practices recommend using AWS Systems Manager Quick Setup for organization-wide management and configuration of EC2 instances. The Default Host Management Configuration Quick Setup automatically enables Systems Manager capabilities such as Patch Manager, Inventory, Session Manager, and Automation across all managed instances within the organization.
When deployed from the management account, Quick Setup automatically integrates with AWS Organizations to propagate configuration and permissions to existing and future accounts. This meets the requirement for organization-wide management with no manual configuration or SSH access. AWS documentation notes:
"You can use Quick Setup in the management account of an organization in AWS Organizations to configure Systems Manager capabilities for all accounts and Regions. Quick Setup automatically keeps configurations up to date." Options B, C, and D require custom deployments or manual IAM updates, lacking centralized automation.
Therefore, Option A fully satisfies CloudOps standards for automated provisioning and ongoing management of EC2 instances

across an organization.
References:* AWS Certified CloudOps Engineer - Associate (SOA-C03) Exam Guide - Domain 3: Deployment, Provisioning and Automation* AWS Systems Manager - Quick Setup and Default Host Management Configuration* AWS Organizations Integration with Systems Manager* AWS Well-Architected Framework - Operational Excellence Pillar

NEW QUESTION # 75
A company observes a dramatic increase in 500 status code responses from an HTTP application that runs on Amazon EC2 instances. The EC2 instances are in an Auto Scaling group and use EC2 health checks for resiliency. The company uses Amazon CloudWatch to collect logs for the EC2 instances and the HTTP server logs.
A CloudOps engineer investigates the cause of the status codes. The CloudOps engineer finds that errors correlate with times when the Auto Scaling group was either replacing EC2 instances or performing scale-in actions. The CloudOps engineer needs to improve the resiliency of the application's architecture.
Which solution will meet this requirement?

- A. Reconfigure the EC2 instance health checks to use Elastic Load Balancing (ELB) health checks.
- B. Reconfigure the EC2 instance health checks to increase the health check grace period.
- C. Reconfigure the Auto Scaling group to increase the default cooldown configuration.
- D. Reconfigure the Auto Scaling group to increase the minimum capacity configuration.

Answer: A

Explanation:
The errors occur during Auto Scaling replacement and scale-in events, which strongly indicates that instances are being terminated or recycled while they are still serving traffic. When an Auto Scaling group uses only EC2 status checks, the health evaluation is limited to instance-level signals (such as system reachability and instance reachability). Those checks do not validate whether the application process is healthy, whether the web server is still responding correctly, or whether the instance is safely able to continue serving requests while shutdown activities are underway. As a result, traffic can continue to reach an instance that is about to be terminated, or a newly launched instance can be marked healthy at the EC2 layer before the application is actually ready, producing spikes in 5xx responses.
Using Elastic Load Balancing health checks integrates the Auto Scaling group with the load balancer's application-aware health evaluation. The load balancer can perform health checks against a specific endpoint (for example, /health) over HTTP/HTTPS and determine whether the application is responding successfully.
Auto Scaling can then replace instances based on real service health rather than only infrastructure health.
This approach improves resiliency because unhealthy or draining instances are removed from load balancing before they cause user-facing errors, and newly launched instances are kept out of rotation until they pass the ELB health checks.
Increasing cooldown (A) only slows scaling actions and does not ensure safe traffic draining. Increasing minimum capacity (C) can reduce impact but does not address the root cause of instances receiving traffic during lifecycle changes. Increasing grace period (D) helps initial warm-up, but it does not reliably protect users during scale-in and termination without application-level health integration.
Therefore, ELB health checks are the best solution.

NEW QUESTION # 76
A CloudOps engineer is responsible for a company's disaster recovery procedures. The company has a source Amazon S3 bucket in a production account, and it wants to replicate objects from the source to a destination S3 bucket in a nonproduction account.
The CloudOps engineer configures S3 cross-Region, cross-account replication to copy the source S3 bucket to the destination S3 bucket. When the CloudOps engineer attempts to access objects in the destination S3 bucket, they receive an Access Denied error.
Which solution will resolve this problem?

- A. Ensure that the replication rule applies to all objects in the source S3 bucket and is not scoped to a single prefix.
- B. Retry the request when the S3 Replication Time Control (S3 RTC) has elapsed.
- C. Modify the replication configuration to change object ownership to the destination S3 bucket owner.
- D. Verify that the storage class for the replicated objects did not change between the source S3 bucket and the destination S3 bucket.

Answer: C

Explanation:
In cross-account S3 replication, a common cause of "Access Denied" when reading replicated objects is object ownership. By default, the replicated objects can remain owned by the source account (the account that originally wrote the objects). Even though the objects are physically stored in the destination bucket, the destination account's users can be blocked from accessing them unless

the correct ACLs or ownership controls are in place. This becomes especially visible in disaster recovery or nonproduction copy scenarios where the destination account expects to independently read and manage replicated data.
Amazon S3 provides an option in replication configuration to change the replica object ownership to the destination bucket owner. When enabled, the destination account becomes the owner of the replicated objects, which aligns access control with the bucket ownership and the destination account's IAM policies.
This removes the common cross-account ownership mismatch and resolves Access Denied errors for legitimate users in the destination account who have permissions on the destination bucket.
Option B relates to which objects are included in replication (prefix scoping). If replication were scoped incorrectly, the symptom would typically be missing objects rather than Access Denied on objects that are present. Option C (S3 RTC) is about replication time guarantees and monitoring; elapsed time does not change ownership or permissions and therefore does not resolve Access Denied. Option D (storage class changes) affects cost and retrieval characteristics, not authorization; it would not typically produce Access Denied for standard reads solely because the storage class differs.
Therefore, updating the replication configuration to ensure replicated objects are owned by the destination bucket owner is the correct fix to restore access.

NEW QUESTION # 77
A CloudOps engineer is troubleshooting an AWS CloudFormation stack creation that failed. Before the CloudOps engineer can identify the problem, the stack and its resources are deleted. For future deployments, the CloudOps engineer must preserve any resources that CloudFormation successfully created.
What should the CloudOps engineer do to meet this requirement?

- A. Specify a rollback configuration that has a rollback trigger of DO_NOTHING during stack creation.
- B. Set the value of the OnFailure parameter to ROLLBACK during stack creation.
- C. Set the value of the OnFailure parameter to DO_NOTHING during stack creation.
- D. Set the value of the DisableRollback parameter to False during stack creation.

Answer: C

Explanation:
By default, when AWS CloudFormation encounters a failure during stack creation, it automatically rolls back and deletes any resources that were successfully created. This behavior makes troubleshooting difficult because the failed and partially created resources are no longer available for inspection.
CloudFormation provides the OnFailure parameter to control this behavior. Setting the parameter to DO_NOTHING instructs CloudFormation to stop stack creation when a failure occurs and retain all successfully created resources. This allows the CloudOps engineer to inspect the environment, review logs, and identify the root cause without redeploying resources.
The DisableRollback parameter controls rollback behavior but does not provide the same explicit behavior control during failure scenarios. Rollback triggers are used for monitoring-based rollback, not for preserving resources on failure. Setting OnFailure to ROLLBACK explicitly enforces deletion, which is the opposite of the requirement.
Therefore, setting the OnFailure parameter to DO_NOTHING is the correct solution.

NEW QUESTION # 78
A company's security policy prohibits connecting to Amazon EC2 instances through SSH and RDP. Instead, staff must use AWS Systems Manager Session Manager. Users report they cannot connect to one Ubuntu instance, even though they can connect to others.
What should a CloudOps engineer do to resolve this issue?

- A. Generate a new key pair, configure Session Manager to use this new key pair, and provide the private key to the users.
- B. Assign the AmazonSSMManagedInstanceCore managed policy to the EC2 instance profile for the Ubuntu instance.
- C. Add an inbound rule for port 22 in the security group associated with the Ubuntu instance.
- D. Configure the SSM Agent to log in with a user name of "ubuntu".

Answer: B

Explanation:
According to AWS Cloud Operations and Systems Manager documentation, Session Manager requires that each managed instance be associated with an IAM instance profile that grants Systems Manager core permissions. The required permissions are provided by the AmazonSSMManagedInstanceCore AWS-managed policy.
If this policy is missing or misconfigured, the Systems Manager Agent (SSM Agent) cannot communicate with the Systems Manager service, causing connection failures even if the agent is installed and running. This explains why other instances work-those instances

likely have the correct IAM role attached.
Enabling port 22 (Option A) violates the company's security policy, while configuring user names (Option C) and key pairs (Option D) are irrelevant because Session Manager operates over secure API channels, not SSH keys.
Therefore, the correct resolution is to attach or update the instance profile with the AmazonSSMManagedInstanceCore policy, restoring Session Manager connectivity.

NEW QUESTION # 79
.....