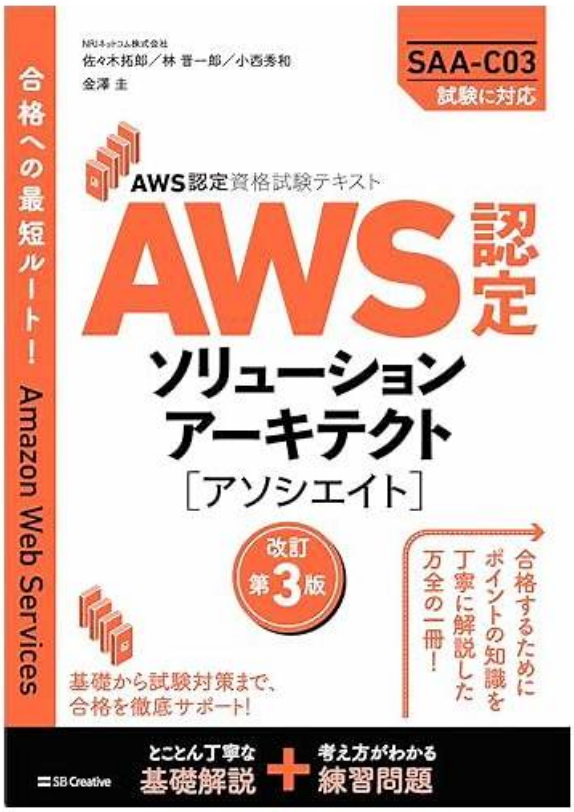
Amazon SOA-C03赤本勉強、SOA-C03受験資料更新版



TopexamのIT認証試験問題集は長年のトレーニング経験を持っています。Topexam AmazonのSOA-C03試験トレーニング資料は信頼できる製品です。当社のスタッフ は受験生の皆様が試験で高い点数を取ることを保証できるように、巨大な努力をして皆様に最新版のSOA-C03試験トレーニング資料を提供しています。Topexam AmazonのSOA-C03試験材料は最も実用的なIT認定材料を提供することを確認することができます。

Amazon SOA-C03 認定試験の出題範囲:

トピック	出題範囲
トピック 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.
トピック 2	• 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.

トピック 3	• 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.
トピック 4	• 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.
トピック 5	• 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.

SOA-C03試験の準備方法｜権威のあるSOA-C03赤本勉強試験｜有難いAWS Certified CloudOps Engineer - Associate受験資料更新版

合格率の高い高品質の最新のSOA-C03認定ガイド資料により、Topexamはどんどん成長しています。過去のデータに基づくと、最近のSOA-C03トレーニングガイドの合格率は最高99％～100％です。多くのお客様は、SOA-C03試験ガイドを一度選択した後、クリアする試験があると、通常の顧客になり、私たちのことを考えます。そのため、宣伝のために多くの精霊を費やす必要はありませんが、研究とアフターサービスのみに力を入れています。 SOA-C03の学習質問で学習する限り、それが正しい選択であることがわかります。

Amazon AWS Certified CloudOps Engineer - Associate 認定 SOA-C03 試験問題 (Q64-Q69):

質問 # 64
An ecommerce company uses Amazon ElastiCache (Redis OSS) for caching product queries.
The CloudOps engineer observes a large number of cache evictions in Amazon CloudWatch metrics and needs to reduce evictions while retaining popular data in cache.
Which solution meets these requirements with the least operational overhead?

- A. Migrate to a new ElastiCache cluster with larger nodes.
- B. Add another node to the ElastiCache cluster.
- C. Increase the ElastiCache TTL value.
- D. Decrease the ElastiCache TTL value.

正解：A

解説：
According to the AWS Cloud Operations and ElastiCache documentation, cache evictions occur when the cache runs out of memory and must remove items to make space for new data.
To reduce evictions and retain frequently accessed items, AWS recommends increasing the total available memory -- either by scaling up to larger node types or scaling out by adding shards/nodes. Migrating to a cluster with larger nodes is the simplest and most efficient solution because it immediately expands capacity without architectural changes.
Adjusting TTL (Options B and C) controls expiration timing, not memory allocation. Adding a single node (Option A) may help, but redistributing data requires resharding, introducing more complexity.
Thus, Option D provides the lowest operational overhead and ensures high cache hit rates by increasing total cache memory.

質問 # 65
A company runs an application on Amazon EC2 instances behind an Elastic Load Balancer (ELB) in an Auto Scaling group. The

application performs well except during a 2-hour period of daily peak traffic, when performance slows.
A CloudOps engineer must resolve this issue with minimal operational effort.
What should the engineer do?

- A. Create a scheduled scaling action to scale out the number of EC2 instances shortly before the increase in user traffic occurs.
- B. Manually add a few more EC2 instances to the Auto Scaling group to support the increase in user traffic. Enable instance scale-in protection on the Auto Scaling group.
- C. Adjust the launch template that is associated with the Auto Scaling group to be more sensitive to increases in user traffic.
- D. Adjust the minimum capacity of the Auto Scaling group to the size required to meet the increased demand during the 2-hour period.

正解：A

解説：
According to the AWS Cloud Operations and Compute documentation, when workloads exhibit predictable traffic patterns, the best practice is to use scheduled scaling for Amazon EC2 Auto Scaling groups.
With scheduled scaling, administrators can predefine the desired capacity of an Auto Scaling group to increase before anticipated demand (in this case, before the 2-hour peak) and scale back down afterward. This ensures that sufficient compute capacity is provisioned proactively, avoiding performance degradation while maintaining cost efficiency.
AWS notes: "Scheduled actions enable scaling your Auto Scaling group at predictable times, allowing you to pre-warm instances before demand spikes." Manual scaling (Option D) adds operational overhead. Adjusting launch templates (Option B) doesn't affect scaling behavior, and permanently increasing minimum capacity (Option A) wastes resources outside of peak hours.
Thus, Option C provides an automated, cost-effective, and operationally efficient CloudOps solution.

質問 # 66
A company runs a retail website on multiple Amazon EC2 instances behind an Application Load Balancer (ALB). The company must secure traffic to the website over an HTTPS connection.
Which combination of actions should a SysOps administrator take to meet these requirements? (Select TWO.)

- A. Create a public certificate in AWS Certificate Manager (ACM).
- B. Create a private certificate in AWS Certificate Manager (ACM).
- C. Export the certificate, and attach it to the website.
- D. Attach the certificate to each EC2 instance.
- E. Attach the certificate to the ALB.

正解：A、E

解説：
Comprehensive and Detailed Explanation From Exact Extract of AWS CloudOps Documents:
To secure inbound web traffic over HTTPS when using an Application Load Balancer, AWS CloudOps best practices recommend terminating TLS at the load balancer. This is achieved by attaching an SSL/TLS certificate directly to the ALB listener. Therefore, option B is required. By terminating HTTPS at the ALB, traffic between clients and the load balancer is encrypted, and the ALB can then forward traffic to backend EC2 instances using HTTP or HTTPS based on design requirements.
The certificate used for a public-facing retail website must be trusted by internet browsers. AWS Certificate Manager (ACM) public certificates are specifically designed for this purpose and are trusted by common browsers and operating systems. Therefore, option D is required. ACM manages certificate provisioning, renewal, and deployment automatically, which significantly reduces operational overhead.
Option A is incorrect because attaching certificates to each EC2 instance is unnecessary and does not scale well. Option C is incorrect because private certificates are intended for internal use cases and are not trusted by public browsers. Option E is incorrect because ACM-managed public certificates cannot be exported; they must be attached directly to supported AWS services such as ALBs.
This approach aligns with AWS CloudOps guidance for secure, scalable, and highly available HTTPS architectures.
References:
Elastic Load Balancing User Guide - HTTPS listeners for Application Load Balancers AWS Certificate Manager User Guide - Public certificates AWS SysOps Administrator Study Guide - Securing applications with ALB and ACM

質問 # 67
A SysOps administrator needs to implement a solution that protects credentials for an Amazon RDS for MySQL DB instance. The

solution must rotate the credentials automatically one time every week.
Which combination of steps will meet these requirements? (Select TWO.)

- A. Create an AWS Lambda function to rotate the credentials.
- B. Configure an RDS proxy to store the credentials.
- C. Add the credentials to AWS Systems Manager Parameter Store.
- D. Add the credentials to AWS Secrets Manager.
- E. Create an AWS Systems Manager Automation runbook to rotate the credentials.

正解：A、D

解説：
Comprehensive and Detailed Explanation From Exact Extract of AWS CloudOps Documents:
The correct answers are B and D. AWS CloudOps documentation clearly states that AWS Secrets Manager is the recommended service for storing and managing database credentials securely. Secrets Manager integrates natively with Amazon RDS and supports automatic, scheduled secret rotation.
To rotate credentials weekly, Secrets Manager requires a Lambda rotation function. AWS provides managed rotation templates for Amazon RDS for MySQL that update the database password and the stored secret atomically. This combination ensures credentials are protected, rotated automatically, and audited with minimal operational effort.
Option A is incorrect because RDS Proxy does not store or rotate credentials; it only retrieves them from Secrets Manager. Option C is incorrect because Systems Manager Parameter Store does not support native automatic rotation. Option E is incorrect because Automation runbooks are not the recommended mechanism for secrets rotation and add unnecessary complexity.
AWS CloudOps best practices strongly recommend Secrets Manager with Lambda-based rotation for database credential protection and compliance.
References:
AWS Secrets Manager User Guide - Automatic Rotation
Amazon RDS User Guide - Credential Management
AWS SysOps Administrator Study Guide - Secrets and Key Management

質問 # 68
A multinational company uses an organization in AWS Organizations to manage over 200 member accounts across multiple AWS Regions. The company must ensure that all AWS resources meet specific security requirements.
The company must not deploy any EC2 instances in the ap-southeast-2 Region. The company must completely block root user actions in all member accounts. The company must prevent any user from deleting AWS CloudTrail logs, including administrators.
The company requires a centrally managed solution that the company can automatically apply to all existing and future accounts.
Which solution will meet these requirements?

- A. Enable AWS Security Hub across the organization. Create custom security standards to enforce the security requirements. Use AWS CloudFormation StackSets to deploy the standards to all the accounts in the organization. Set up Security Hub automated remediation actions.
- B. Create AWS Config rules with remediation actions in each account to detect policy violations.
  Implement IAM permissions boundaries for the account root users.
- C. Use AWS Control Tower for account governance. Configure Region deny controls. Use Service Control Policies (SCPs) to restrict root user access.
- D. Configure AWS Firewall Manager with security policies to meet the security requirements. Use an AWS Config aggregator with organization-wide conformance packs to detect security policy violations.

正解：C

解説：
AWS CloudOps governance best practices emphasize centralized account management and preventive guardrails. AWS Control Tower integrates directly with AWS Organizations and provides "Region deny controls" and "Service Control Policies (SCPs)" that apply automatically to all existing and newly created member accounts. SCPs are organization-wide guardrails that define the maximum permissions for accounts. They can explicitly deny actions such as launching EC2 instances in a specific Region, or block root user access.
To prevent CloudTrail log deletion, SCPs can also include denies on cloudtrail:DeleteTrail and s3:
DeleteObject actions targeting the CloudTrail log S3 bucket. These SCPs ensure that no user, including administrators, can violate the compliance requirements.
AWS documentation under the Security and Compliance domain for CloudOps states:
"Use AWS Control Tower to establish a secure, compliant, multi-account environment with preventive guardrails through service

control policies and detective controls through AWS Config." This approach meets all stated needs: centralized enforcement, automatic propagation to new accounts, region- based restrictions, and immutable audit logs. Options A, B, and D either detect violations reactively or lack complete enforcement and automation across future accounts.
References:* AWS Certified CloudOps Engineer - Associate (SOA-C03) Exam Guide - Domain 4: Security and Compliance* AWS Control Tower - Preventive and Detective Guardrails* AWS Organizations - Service Control Policies (SCPs)* AWS Well-Architected Framework - Security Pillar (Governance and Centralized Controls)

質問 # 69
.....

弊社TopexamのSOA-C03試験準備では、学習習慣を身に付けるのに役立ちます。 SOA-C03学習教材を購入して使用すると、学習の良い習慣を身に付けることができます。さらに重要なことは、良い習慣は科学的な小道具の学習方法を見つけ、学習効率を高めるのに役立ちます。そして、短時間でSOA-C03試験に合格するのに役立ちます。弊社からSOA-C03テストガイドを急いで購入すると、多くのメリットが得られます。