# Introduction

The AWS Certified SysOps Administrator – Associate (SOA-C02) examination is intended for system administrators in a cloud operations role who have at least 1 year of hands-on experience with deployment, management, networking, and security on AWS.

The exam validates an examinee's ability to:

- Deploy, manage, and operate workloads on AWS
- Support and maintain AWS workloads according to the AWS Well-Architected Framework
- Perform operations by using the AWS Management Console and the AWS CLI
- Implement security controls to meet compliance requirements
- Monitor, log, and troubleshoot systems
- Apply networking concepts (for example, DNS, TCP/IP, firewalls)
- Implement architectural requirements (for example, high availability, performance, capacity)
- Perform business continuity and disaster recovery procedures
- Identify, classify, and remediate incidents

**Recommended AWS Knowledge**

- Minimum of 1 year of hands-on experience with AWS technology
- Experience in deploying, managing, and operating workloads on AWS
- Understanding of the AWS Well-Architected Framework
- Hands-on experience with the AWS Management Console and the AWS CLI
- Understanding of AWS networking and security services
- Hands-on experience in implementing security controls and compliance requirements

# Exam Content

**Response Types**
There may be three types of questions on the examination. Some, or all, of these question types may be present during your exam.

- **Multiple choice:** Has one correct response and three incorrect responses (distractors).
- **Multiple response:** Has two correct responses out of five options.
- **Exam lab:** Has a scenario that is composed of a set of tasks to perform in the AWS Management Console or AWS CLI.

**Multiple choice and multiple response:** Select one or more responses that best complete the statement or answer the question. Distractors, or incorrect answers, are response options that an examinee with incomplete knowledge or skill would likely choose. However, they are generally plausible responses that fit in the content area defined by the test objective.

Unanswered questions are scored as incorrect; there is no penalty for guessing.

All multiple choice and multiple response questions will be presented at the start of the exam in one section. There will be a review screen at the end of this section, where you may return to any of the multiple choice and multiple response questions. This will be the last opportunity to answer or change any multiple choice or multiple response selections. If your exam contains exam labs, that section will be presented after the multiple choice and multiple response section. You will NOT be able to go back to the first section after you start the second section.

**Exam labs:** Complete the required tasks for a given scenario in the AWS Management Console or AWS CLI in the provided AWS account.

When you begin your exam, you will be notified of the number of questions in the multiple choice and multiple response section, and the number of exam labs in the exam lab section. You will also see the percentage of your score that will be determined by your work in the exam labs. Plan to leave 20 minutes to complete each exam lab.

Finish all work on an exam lab before moving to the next one. You will NOT be able to return to a prior exam lab. You are welcome to use the virtual machine notepad or AWS CLI while working on your exam labs.

There may be more than one way to perform an exam lab. In those cases, a full score will be awarded if the correct end state to the scenario is achieved. Partial credit is awarded for partial completion of exam labs. However, exam content and the associated scoring are confidential, so no further information can be provided regarding partial credit awarded for an exam lab.

> Tip: If you take your exam through online proctoring, you are permitted to use an external monitor as your ONLY display. Please set your screen resolution to 1,920 x 1,080 or 1,280 x 1,024. Set the scaling to 100%. Other settings may result in scrolling within the console.

For a sample of the multiple choice and multiple response questions and exam labs, please view the AWS Certified SysOps Administrator – Associate (SOA-C02) Sample Exam Questions document.

**Unscored Content**
Your examination may include unscored questions that are placed on the test to gather statistical information. These questions are not identified on the form and do not affect your score.

**Exam Results**
The AWS Certified SysOps Administrator – Associate (SOA-C02) examination is a pass or fail exam. The examination is scored against a minimum standard established by AWS professionals who are guided by certification industry best practices and guidelines.

Your results for the examination are reported as a score from 100–1,000, with a minimum passing score of 720. Your score shows how you performed on the examination as a whole and whether or not you passed. Scaled scoring models are used to equate scores across multiple exam forms that may have slightly different difficulty levels.

Your score report contains a table of classifications of your performance at each section level. This information is designed to provide general feedback concerning your examination performance. The examination uses a compensatory scoring model, which means that you do not need to "pass" the individual sections, only the overall examination. Each section of the examination has a specific weighting, so some sections have more questions than others. The table contains general information, highlighting your strengths and weaknesses. Exercise caution when interpreting section-level feedback.

**Content Outline**
This exam guide includes weightings, test domains, objectives, and example tasks only. It is not a comprehensive listing of the content on this examination. The table below lists the main content domains and their weightings.

| Domain | % of Examination |
|---|---|
| Domain 1: Monitoring, Logging, and Remediation | 20% |
| Domain 2: Reliability and Business Continuity | 16% |
| Domain 3: Deployment, Provisioning, and Automation | 18% |
| Domain 4: Security and Compliance | 16% |
| Domain 5: Networking and Content Delivery | 18% |
| Domain 6: Cost and Performance Optimization | 12% |
| **TOTAL** | **100%** |

**Domain 1: Monitoring, Logging, and Remediation**

    1.1  Implement metrics, alarms, and filters by using AWS monitoring and logging services
- Identify, collect, analyze, and export logs (for example, Amazon CloudWatch Logs, CloudWatch Logs Insights, AWS CloudTrail logs)
- Collect metrics and logs using the CloudWatch agent
- Create CloudWatch alarms
- Create metric filters
- Create  CloudWatch dashboards
- Configure notifications (for example, Amazon Simple Notification Service [Amazon SNS], Service Quotas, CloudWatch alarms, AWS Health events)

    1.2  Remediate issues based on monitoring and availability metrics
- Troubleshoot or take corrective actions based on notifications and alarms
- Configure Amazon EventBridge rules to trigger actions
- Use AWS Systems Manager Automation documents to take action based on AWS Config rules

**Domain 2: Reliability and Business Continuity**

    2.1  Implement scalability and elasticity
- Create and maintain AWS Auto Scaling plans
- Implement caching
- Implement Amazon RDS replicas and Amazon Aurora Replicas
- Implement loosely coupled architectures
- Differentiate between horizontal scaling and vertical scaling

    2.2  Implement high availability and resilient environments
- Configure Elastic Load Balancer and Amazon Route 53 health checks
- Differentiate between the use of a single Availability Zone and Multi-AZ deployments (for example, Amazon EC2 Auto Scaling groups, Elastic Load Balancing, Amazon FSx, Amazon RDS)
- Implement fault-tolerant workloads (for example, Amazon Elastic File System [Amazon EFS], Elastic IP addresses)
- Implement Route 53 routing policies (for example, failover, weighted, latency based)

    2.3  Implement backup and restore strategies
- Automate snapshots and backups based on use cases (for example, RDS snapshots, AWS Backup, RTO and RPO, Amazon Data Lifecycle Manager, retention policy)
- Restore databases (for example, point-in-time restore, promote read replica)
- Implement versioning and lifecycle rules
- Configure Amazon S3 Cross-Region Replication
- Execute disaster recovery procedures

**Domain 3: Deployment, Provisioning, and Automation**

    3.1  Provision and maintain cloud resources
- Create and manage AMIs (for example, EC2 Image Builder)
- Create, manage, and troubleshoot AWS CloudFormation
- Provision resources across multiple AWS Regions and accounts (for example, AWS Resource Access Manager, CloudFormation StackSets, IAM cross-account roles)
- Select deployment scenarios and services (for example, blue/green, rolling, canary)
- Identify and remediate deployment issues (for example, service quotas, subnet sizing, CloudFormation and AWS OpsWorks errors, permissions)

    3.2  Automate manual or repeatable processes
- Use AWS services (for example, OpsWorks, Systems Manager, CloudFormation) to automate deployment processes
- Implement automated patch management
- Schedule automated tasks by using AWS services (for example, EventBridge, AWS Config)

**Domain 4: Security and Compliance**

    4.1  Implement and manage security and compliance policies

- Implement IAM features (for example, password policies, MFA, roles, SAML, federated identity, resource policies, policy conditions)
- Troubleshoot and audit access issues by using AWS services (for example, CloudTrail, IAM Access Analyzer, IAM policy simulator)
- Validate service control policies and permission boundaries
- Review AWS Trusted Advisor security checks
- Validate AWS Region and service selections based on compliance requirements
- Implement secure multi-account strategies (for example, AWS Control Tower, AWS Organizations)

4.2 Implement data and infrastructure protection strategies
- Enforce a data classification scheme
- Create, manage, and protect encryption keys
- Implement encryption at rest (for example, AWS Key Management Service [AWS KMS])
- Implement encryption in transit (for example, AWS Certificate Manager, VPN)
- Securely store secrets by using AWS services (for example, AWS Secrets Manager, Systems Manager Parameter Store)
- Review reports or findings (for example, AWS Security Hub, Amazon GuardDuty, AWS Config, Amazon Inspector)

## Domain 5: Networking and Content Delivery

5.1 Implement networking features and connectivity
- Configure a VPC (for example, subnets, route tables, network ACLs, security groups, NAT gateway, internet gateway )
- Configure private connectivity (for example, Systems Manager Session Manager, VPC endpoints, VPC peering, VPN)
- Configure AWS network protection services (for example, AWS WAF, AWS Shield)

5.2 Configure domains, DNS services, and content delivery
- Configure Route 53 hosted zones and records
- Implement Route 53 routing policies (for example, geolocation, geoproximity)
- Configure DNS (for example, Route 53 Resolver)
- Configure Amazon CloudFront and S3 origin access identity (OAI)
- Configure S3 static website hosting

5.3 Troubleshoot network connectivity issues
- Interpret VPC configurations (for example, subnets, route tables, network ACLs, security groups)
- Collect and interpret logs (for example, VPC Flow Logs, Elastic Load Balancer access logs, AWS WAF web ACL logs, CloudFront logs)
- Identify and remediate CloudFront caching issues
- Troubleshoot hybrid and private connectivity issues

## Domain 6: Cost and Performance Optimization

6.1 Implement cost optimization strategies
- Implement cost allocation tags
- Identify and remediate underutilized or unused resources by using AWS services and tools (for example, Trusted Advisor, AWS Compute Optimizer, Cost Explorer)
- Configure AWS Budgets and billing alarms
- Assess resource usage patterns to qualify workloads for EC2 Spot Instances
- Identify opportunities to use managed services (for example, Amazon RDS, AWS Fargate, EFS)

6.2 Implement performance optimization strategies
- Recommend compute resources based on performance metrics
- Monitor Amazon EBS metrics and modify configuration to increase performance efficiency
- Implement S3 performance features (for example, S3 Transfer Acceleration, multipart uploads)
- Monitor RDS metrics and modify the configuration to increase performance efficiency (for example, performance insights, RDS Proxy)
- Enable enhanced EC2 capabilities (for example, enhanced network adapter, instance store, placement groups)