aws training and certification

AWS Certified SysOps Administrator – Associate (SOA-C02) Exam Guide

Introduction

The AWS Certified SysOps Administrator – Associate (SOA-C02) exam is intended for system administrators in a cloud operations role. The exam validates a candidate's ability to deploy, manage, and operate workloads on AWS.

The exam also validates a candidate's ability to complete the following tasks:

- 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

Target candidate description

The target candidate should have 1 year of experience with deployment, management, networking, and security on AWS.

Recommended general IT knowledge

The target candidate should have the following knowledge:

- 1–2 years of experience as a systems administrator in an operations role
- Experience in monitoring, logging, and troubleshooting
- Knowledge of networking concepts (for example, DNS, TCP/IP, firewalls)
- Ability to implement architectural requirements (for example, high availability, performance, capacity)

Recommended AWS knowledge

The target candidate should have the following 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

What is considered out of scope for the target candidate?

The following is a non-exhaustive list of related job tasks that the target candidate is not expected to be able to perform. These items are considered out of scope for the exam:

- Design distributed architectures
- Design continuous integration and continuous delivery (CI/CD) pipelines
- Design hybrid and multi-VPC networking
- Develop software
- Define security, compliance, and governance requirements

For a detailed list of specific tools and technologies that might be covered on the exam, as well as lists of in-scope and out-of-scope AWS services, refer to the Appendix.

Exam content

Response types

There are three types of questions on the exam:

- **Multiple choice:** Has one correct response and three incorrect responses
- **Multiple response:** Has two or more correct responses out of five or more response 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 a candidate with incomplete knowledge or skill might choose. Distractors are generally plausible responses that match the content area.

All multiple-choice and multiple-response questions will appear at the start of the exam in one section. The end of this section will include a review screen, where you can return to any of the multiple-choice and multiple-response questions. This will be the last opportunity to answer the questions or change any answer selections. If your exam contains exam labs, that section will appear 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 receive notification about 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 learn 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 you move to the next exam lab. 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 might be more than one way to perform an exam lab. In those cases, you will receive full credit if you achieve the correct end state to the scenario. You will receive partial credit for partial completion of

exam labs. However, exam content and the associated scoring are confidential, so you will receive no further information regarding partial credit that is awarded for an exam lab.

> Tip: If you take your exam through online proctoring, you can use an external monitor as your ONLY display. Set your screen resolution to 1280 pixels x 1024 pixels or greater for a PC, and 1440 pixels x 900 pixels or greater for a Mac. Set the scaling to 100%. Other settings might result in a need to scroll within the console.

On the exam, unanswered questions are scored as incorrect; there is no penalty for guessing. The exam includes 50 questions that affect your score. These questions include multiple-choice questions, multiple-response questions, and exam labs. Each scored multiple-choice question and each scored multiple-response question counts as a single scored opportunity. A scored exam lab includes multiple scored opportunities.

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

Unscored content

The exam includes 15 unscored questions that do not affect your score. AWS collects information about candidate performance on these unscored questions to evaluate these questions for future use as scored questions. These unscored questions are not identified on the exam.

Exam results

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

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

Your score report may contain a table of classifications of your performance at each section level. This information is intended to provide general feedback about your exam performance. The exam uses a compensatory scoring model, which means that you do not need to achieve a passing score in each section. You need to pass only the overall exam.

Each section of the exam has a specific weighting, so some sections have more questions than other sections have. The table contains general information that highlights your strengths and weaknesses. Use caution when interpreting section-level feedback.

Content outline

This exam guide includes weightings, test domains, and objectives for the exam. It is not a comprehensive listing of the content on the exam. However, additional context for each of the objectives is available to help guide your preparation for the exam. The following table lists the main content domains and their weightings. The table precedes the complete exam content outline, which includes the additional context. The percentage in each domain represents only scored content.

Domain	% of Exam
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 permissions 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)

Appendix

Which key tools, technologies, and concepts might be covered on the exam?

The following is a non-exhaustive list of the tools and technologies that could appear on the exam. This list is subject to change and is provided to help you understand the general scope of services, features, or technologies on the exam. The general tools and technologies in this list appear in no particular order. AWS services are grouped according to their primary functions. While some of these technologies will likely be covered more than others on the exam, the order and placement of them in this list is no indication of relative weight or importance:

- Analytics
- Application Integration
- AWS Cost Management
- Compute
- Containers
- Database
- Management, Monitoring, and Governance
- Migration and Transfer
- Networking and Content Delivery
- Security, Identity, and Compliance
- Storage

AWS services and features

Analytics:

- Amazon Elasticsearch Service (Amazon ES)

Application Integration:

- Amazon EventBridge (Amazon CloudWatch Events)
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Queue Service (Amazon SQS)

AWS Cost Management:

- AWS Cost and Usage Report
- AWS Cost Explorer
- Savings Plans

Compute:

- AWS Application Auto Scaling
- Amazon EC2
- Amazon EC2 Auto Scaling
- Amazon EC2 Image Builder
- AWS Lambda

Database:

- Amazon Aurora
- Amazon ElastiCache
- Amazon RDS

Management, Monitoring, and Governance:

- AWS CloudFormation
- AWS CloudTrail
- Amazon CloudWatch
- AWS Command Line Interface (AWS CLI)
- AWS Compute Optimizer
- AWS Config
- AWS Control Tower
- AWS License Manager
- AWS Management Console
- AWS OpsWorks
- AWS Organizations
- AWS Personal Health Dashboard
- AWS Secrets Manager
- AWS Service Catalog
- AWS Systems Manager
- AWS Systems Manager Parameter Store
- AWS tools and SDKs
- AWS Trusted Advisor

Migration and Transfer:

- AWS DataSync
- AWS Transfer Family

Networking and Content Delivery:

- AWS Client VPN
- Amazon CloudFront
- Elastic Load Balancing
- AWS Firewall Manager
- AWS Global Accelerator
- Amazon Route 53
- Amazon Route 53 Resolver
- AWS Transit Gateway
- Amazon VPC
- Amazon VPC Traffic Mirroring

Security, Identity, and Compliance:

- AWS Certificate Manager (ACM)
- Amazon Detective
- AWS Directory Service
- Amazon GuardDuty
- AWS IAM Access Analyzer
- AWS Identity and Access Management (IAM)
- Amazon Inspector
- AWS Key Management Service (AWS KMS)
- AWS License Manager
- AWS Secrets Manager
- AWS Security Hub

- AWS Shield
- AWS WAF

Storage:

- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic File System (Amazon EFS)
- Amazon FSx
- Amazon S3
- Amazon S3 Glacier
- AWS Backup
- AWS Storage Gateway

Out-of-scope AWS services and features

The following is a non-exhaustive list of AWS services and features that are not covered on the exam. These services and features do not represent every AWS offering that is excluded from the exam content. Services or features that are entirely unrelated to the target job roles for the exam are excluded from this list because they are assumed to be irrelevant.

Out-of-scope AWS services and features include the following:

- Amazon API Gateway
- Amazon AppStream 2.0
- AWS Batch
- Amazon Chime
- Amazon Cloud Directory
- Amazon CloudSearch
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodeStar
- Amazon Connect
- AWS Deep Learning AMIs (DLAMI)
- AWS Device Farm
- Amazon DynamoDB
- Amazon DynamoDB Accelerator (DAX)
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)
- Amazon Elastic Transcoder
- Amazon EMR
- Amazon GameLift
- AWS IoT Button
- AWS IoT Greengrass
- AWS IoT Platform
- Amazon Kinesis
- Amazon Lex
- Amazon Lightsail
- Amazon Lumberyard
- Amazon Machine Learning (Amazon ML)

- AWS Managed Services
- AWS Mobile Hub
- AWS Mobile SDK
- Apache MXNet on AWS
- Amazon Pinpoint
- Amazon Polly
- Amazon Redshift
- Amazon Rekognition
- AWS Schema Conversion Tool
- Amazon Simple Email Service (Amazon SES)
- AWS Snowmobile
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS X-Ray