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 and experience

The target candidate should have the following general IT knowledge and experience:

- 1–2 years of experience as a system 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 and experience

The target candidate should have the following AWS knowledge and experience:

- 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

Job tasks that are out of scope for the target candidate

The following list contains job tasks that the target candidate is not expected to be able to perform. This list is non-exhaustive. These tasks are 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.

Refer to the Appendix for a list of in-scope AWS services and features and a list of out-of-scope AWS services and features.

Exam content

Response types

As of March 28, 2023, the exam will consist of two types of questions until further notice:

- **Multiple choice:** Has one correct response and three incorrect responses (distractors)
- **Multiple response:** Has two or more correct responses out of five or more response options

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.

NOTE: As of March 28, 2023, the AWS Certified SysOps Administrator - Associate exam will not include exam labs until further notice. This removal of exam labs is temporary while we evaluate the exam labs and make improvements to provide an optimal candidate experience. With this change, the exam will consist of 50 scored and 15 unscored multiple-choice questions and multiple-response questions, with an exam time of 130 minutes. All exam prep resources that are available on the exam page remain valid for this changed exam format.

- **Exam lab:** Has a scenario that is composed of a set of tasks to perform in the AWS Management Console or AWS CLI

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 allocate 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 questions, 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 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 has a pass or fail designation. 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 you passed. Scaled scoring models help equate scores across multiple exam forms that might have slightly different difficulty levels.

Your score report could contain a table of classifications of your performance at each section level. 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 of classifications contains general information that highlights your strengths and weaknesses. Use caution when you interpret section-level feedback.

Content outline

This exam guide includes weightings, content domains, and task statements for the exam. This guide does not provide a comprehensive list of the content on the exam. However, additional context for each task statement is available to help you prepare for the exam.

The exam has the following content domains and weightings:

- Domain 1: Monitoring, Logging, and Remediation (20% of scored content)
- Domain 2: Reliability and Business Continuity (16% of scored content)
- Domain 3: Deployment, Provisioning, and Automation (18% of scored content)
- Domain 4: Security and Compliance (16% of scored content)
- Domain 5: Networking and Content Delivery (18% of scored content)
- Domain 6: Cost and Performance Optimization (12% of scored content)

Domain 1: Monitoring, Logging, and Remediation

Task Statement 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 by 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).

Task Statement 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 invoke actions.
- Use AWS Systems Manager Automation runbooks to take action based on AWS Config rules.

Domain 2: Reliability and Business Continuity

Task Statement 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.

Task Statement 2.2: Implement high availability and resilient environments.

- Configure Elastic Load Balancing (ELB) 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, ELB, 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).

Task Statement 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 (CRR).
- Perform disaster recovery procedures.

Domain 3: Deployment, Provisioning, and Automation

Task Statement 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 [AWS RAM], 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 errors, permissions).

Task Statement 3.2: Automate manual or repeatable processes.

- Use AWS services (for example, 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

Task Statement 4.1: Implement and manage security and compliance policies.

- Implement IAM features (for example, password policies, multi-factor authentication [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 (SCPs) 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).

Task Statement 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 [ACM], 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

Task Statement 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).

Task Statement 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 control (OAC).
- Configure S3 static website hosting.

Task Statement 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, ELB 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

Task Statement 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, AWS 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, Amazon EFS).

Task Statement 6.2: Implement performance optimization strategies.

- Recommend compute resources based on performance metrics.
- Monitor Amazon Elastic Block Store (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, Elastic Network Adapter, instance store, placement groups).

Appendix

In-scope AWS services and features

The following list contains AWS services and features that are in scope for the exam. This list is non-exhaustive and is subject to change. AWS offerings appear in categories that align with the offerings' primary functions:

Analytics:

- Amazon OpenSearch Service

Application Integration:

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

Cloud Financial Management:

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

Compute:

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

Database:

- Amazon Aurora
- Amazon DynamoDB
- Amazon ElastiCache
- Amazon RDS

Developer Tools:

- AWS tools and SDKs

Management and Governance:

- AWS CLI
- AWS CloudFormation
- AWS CloudTrail
- Amazon CloudWatch
- AWS Compute Optimizer
- AWS Config
- AWS Control Tower
- AWS Health Dashboard
- AWS License Manager
- AWS Management Console
- AWS Organizations
- AWS Service Catalog
- AWS Systems Manager
- AWS Trusted Advisor

Migration and Transfer:

- AWS DataSync
- AWS Transfer Family

Networking and Content Delivery:

- Amazon CloudFront
- Elastic Load Balancing (ELB)
- AWS Global Accelerator
- Amazon Route 53
- AWS Transit Gateway
- Amazon VPC
- AWS VPN

Security, Identity, and Compliance:

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

Storage:

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

Out-of-scope AWS services and features

The following list contains AWS services and features that are out of scope for the exam. This list is non-exhaustive and is subject to change. AWS offerings that are entirely unrelated to the target job roles for the exam are excluded from this list:

Analytics:

- Amazon EMR

Business Applications:

- Amazon Chime
- Amazon Connect
- Amazon WorkDocs
- Amazon WorkMail

Compute:

- Amazon Lightsail

Containers:

- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)

Database:

- Amazon Redshift

Developer Tools:

- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodeStar
- AWS X-Ray

End User Computing:

- Amazon AppStream 2.0
- Amazon WorkSpaces

Frontend Web and Mobile:

- AWS Device Farm
- AWS Mobile SDKs
- Amazon Pinpoint

Game Tech:

- Amazon GameLift

Internet of Things (IoT):

- AWS IoT Button
- AWS IoT Greengrass
- AWS IoT Platform

Machine Learning:

- AWS Deep Learning AMIs (DLAMI)
- Amazon Lex
- Amazon Lumberyard
- Amazon Machine Learning (Amazon ML)
- Apache MXNet on AWS
- Amazon Polly
- Amazon Rekognition

Management and Governance:

- AWS Managed Services (AMS)

Media Services:

- Amazon Elastic Transcoder

Migration and Transfer:

- AWS Schema Conversion Tool (AWS SCT)

Security, Identity, and Compliance:

- Amazon Cloud Directory

Storage:

- AWS Snowmobile

Survey

How useful was this exam guide? Let us know by taking our survey.