AWS Certified CloudOps Engineer - Associate (SOA-C03) Exam Guide

Introduction

The AWS Certified CloudOps Engineer - Associate (SOA-C03) exam is intended for CloudOps engineers. 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, troubleshooting, networking, and security on AWS. The target candidate also should have at least 1 year of experience in a related operations role such as system administrator.

Recommended general IT knowledge and experience

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

- Techniques for monitoring, logging, and troubleshooting
- Networking concepts (for example, DNS, TCP, IP, firewalls)
- Implementation of architectural requirements (for example, high availability, performance, capacity)
- Familiarity with at least one scripting language
- Familiarity with at least one major operating system

- Understanding of cloud computing
- Containerization and orchestration basics
- Understanding of continuous integration and continuous delivery (CI/CD) and Git

Recommended AWS knowledge and experience

The target candidate should have the following AWS knowledge:

- The AWS Well-Architected Framework
- AWS storage and container solutions
- AWS monitoring tools
- How to use the AWS Management Console, the AWS CLI, infrastructure as code (IaC) solutions, and AWS CloudFormation
- AWS networking and security services
- How to implement AWS security controls and compliance requirements
- Cloud financial management
- Operations within hybrid and multi-VPC environments
- AWS database services (for example, Amazon RDS, Amazon DynamoDB, Amazon ElastiCache)
- AWS compute services (for example, Amazon EC2, AWS Lambda, Amazon Elastic Container Service [Amazon ECS])

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 CI/CD pipelines.
- Design hybrid and multi-VPC networking.
- Develop software.
- Define security, compliance, and governance requirements.
- Develop ransomware defense strategies.
- Assess and plan resource capacity.
- Analyze costs and total cost of ownership.
- Manage billing and invoicing for AWS services.

Refer to Appendix A 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

The exam includes two types of questions:

- **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.

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 and multiple-response questions. Each scored multiple-choice question and each scored multiple-response question counts as a single scored opportunity.

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 CloudOps Engineer - Associate (SOA-C03) 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:

- Content Domain 1: Monitoring, Logging, Analysis, Remediation, and Performance Optimization (22% of scored content)
- Content Domain 2: Reliability and Business Continuity (22% of scored content)
- Content Domain 3: Deployment, Provisioning, and Automation (22% of scored content)
- Content Domain 4: Security and Compliance (16% of scored content)
- Content Domain 5: Networking and Content Delivery (18% of scored content)

Content Domain 1: Monitoring, Logging, Analysis, Remediation, and Performance Optimization

Task 1.1: Implement metrics, alarms, and filters by using AWS monitoring and logging services.

- Skill 1.1.1: Configure AWS monitoring and logging by using AWS services (for example, Amazon CloudWatch, AWS CloudTrail, Amazon Managed Service for Prometheus).
- Skill 1.1.2: Configure and manage the CloudWatch agent to collect metrics and logs from EC2 instances, Amazon ECS clusters, or Amazon Elastic Kubernetes Service (Amazon EKS) clusters.
- Skill 1.1.3: Configure, identify, and troubleshoot CloudWatch alarms that can invoke AWS services directly or through Amazon EventBridge (for example, by creating composite alarms and identifying their invokable actions).
- Skill 1.1.4: Create, implement, and manage customizable and shareable CloudWatch dashboards that display metrics and alarms for AWS resources across multiple accounts and AWS Regions.
- Skill 1.1.5: Configure AWS services to send notifications to Amazon Simple Notification Service (Amazon SNS) and to invoke alarms that send notifications to Amazon SNS.

Task 1.2: Identify and remediate issues by using monitoring and availability metrics.

- Skill 1.2.1: Analyze performance metrics and automate remediation strategies by using AWS services and functionality (for example, CloudWatch, AWS User Notifications, Lambda, Systems Manager, CloudTrail, auto scaling).
- Skill 1.2.2: Use EventBridge to route, enrich, and deliver events, and troubleshoot any issues with event bus rules.
- Skill 1.2.3: Create or run custom and predefined Systems Manager Automation runbooks (for example, by using AWS SDKs or custom scripts) to automate tasks and streamline processes on AWS.

Task 1.3: Implement performance optimization strategies for compute, storage, and database resources.

- Skill 1.3.1: Optimize compute resources and remediate performance problems by using performance metrics, resource tags, and AWS tools.
- Skill 1.3.2: Analyze Amazon Elastic Block Store (Amazon EBS) performance metrics, troubleshoot issues, and optimize volume types to improve performance and reduce cost.
- Skill 1.3.3: Implement and optimize S3 performance strategies (for example, AWS DataSync, S3 Transfer Acceleration, multipart uploads, S3 Lifecycle policies) to enhance data transfer, storage efficiency, and access patterns.
- Skill 1.3.4: Evaluate and select shared storage solutions (for example, Amazon Elastic File System [Amazon EFS], Amazon FSx), and optimize the solutions (for example, EFS lifecycle policies) for specific use cases and requirements.
- Skill 1.3.5: Monitor Amazon RDS metrics (for example, Amazon RDS Performance Insights, CloudWatch alarms), and modify configurations to increase performance efficiency (for example, Performance Insights proactive recommendations, RDS Proxy).
- Skill 1.3.6: Implement, monitor, and optimize EC2 instances and their associated storage and networking capabilities (for example, EC2 placement groups).

Content Domain 2: Reliability and Business Continuity

Task 2.1: Implement scalability and elasticity.

- Skill 2.1.1: Configure and manage scaling mechanisms in compute environments.
- Skill 2.1.2: Implement caching by using AWS services to enhance dynamic scalability (for example, CloudFront, Amazon ElastiCache).
- Skill 2.1.3: Configure and manage scaling in AWS managed databases (for example, Amazon RDS, DynamoDB).

Task 2.2: Implement highly available and resilient environments.

- Skill 2.2.1: Configure and troubleshoot Elastic Load Balancing (ELB) and Amazon Route 53 health checks.
- Skill 2.2.2: Configure fault-tolerant systems (for example, Multi-AZ deployments).

Task 2.3: Implement backup and restore strategies.

- Skill 2.3.1: Automate snapshots and backups for AWS resources (for example, EC2 instances, RDS DB instances, EBS volumes, S3 buckets, DynamoDB tables) by using AWS services (for example, AWS Backup).
- Skill 2.3.2: Use various methods to restore databases (for example, point-in-time restore) to meet recovery time objective (RTO), recovery point objective (RPO), and cost requirements.
- Skill 2.3.3: Implement versioning for storage services (for example, Amazon S3, Amazon FSx).
- Skill 2.3.4: Follow disaster recovery procedures.

Content Domain 3: Deployment, Provisioning, and Automation

Task 3.1: Provision and maintain cloud resources.

- Skill 3.1.1: Create and manage AMIs and container images (for example, EC2 Image Builder).
- Skill 3.1.2: Create and manage stacks of resources by using CloudFormation and the AWS Cloud Development Kit (AWS CDK).
- Skill 3.1.3: Identify and remediate deployment issues (for example, subnet sizing issues, CloudFormation errors, permissions issues).
- Skill 3.1.4: Provision and share resources across multiple Regions and accounts (for example, AWS Resource Access Manager [AWS RAM], CloudFormation StackSets).
- Skill 3.1.5: Implement deployment strategies and services.
- Skill 3.1.6: Use and manage third-party tools to automate resource deployment (for example, Terraform, Git).

Task 3.2: Automate the management of existing resources.

- Skill 3.2.1: Use AWS services to automate operational processes (for example, Systems Manager).
- Skill 3.2.2: Implement event-driven automation by using AWS services and features (for example, Lambda, S3 Event Notifications).

Content Domain 4: Security and Compliance

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

- Skill 4.1.1: Implement AWS Identity and Access Management (IAM) features (for example, password policies, multi-factor authentication [MFA], roles, federated identity, resource policies, policy conditions).
- Skill 4.1.2: Troubleshoot and audit access issues by using AWS tools (for example, CloudTrail, IAM Access Analyzer, IAM policy simulator).
- Skill 4.1.3: Implement multi-account strategies securely.
- Skill 4.1.4: Implement remediation based on the results of AWS Trusted Advisor security checks.
- Skill 4.1.5: Enforce compliance requirements (for example, Region and service selections).

Task 4.2: Implement strategies to protect data and infrastructure.

- Skill 4.2.1: Implement and enforce a data classification scheme.
- Skill 4.2.2: Implement, configure, and troubleshoot encryption at rest (for example, AWS Key Management Service [AWS KMS]).
- Skill 4.2.3: Implement, configure, and troubleshoot encryption in transit (for example, AWS Certificate Manager [ACM]).
- Skill 4.2.4: Securely store secrets by using AWS services.
- Skill 4.2.5: Configure reports and remediate findings from AWS services (for example, Security Hub, Amazon GuardDuty, AWS Config, Amazon Inspector).

Content Domain 5: Networking and Content Delivery

Task 5.1: Implement and optimize networking features and connectivity.

- Skill 5.1.1: Configure a VPC (for example, subnets, route tables, network ACLs, security groups, NAT gateways, internet gateway, egress-only internet gateway).
- Skill 5.1.2: Configure private networking connectivity.
- Skill 5.1.3: Audit AWS network protection services (for example, Route 53 Resolver DNS Firewall, AWS WAF, AWS Shield, AWS Network Firewall) in a single account.
- Skill 5.1.4: Optimize the cost of network architectures.

Task 5.2: Configure domains, DNS services, and content delivery.

- Skill 5.2.1: Configure DNS (for example, Route 53 Resolver).
- Skill 5.2.2: Implement Route 53 routing policies, configurations, and query logging.
- Skill 5.2.3: Configure content and service distribution (for example, CloudFront, AWS Global Accelerator).

Task 5.3: Troubleshoot network connectivity issues.

- Skill 5.3.1: Troubleshoot VPC configurations (for example, subnets, route tables, network ACLs, security groups, transit gateways, NAT gateways).
- Skill 5.3.2: Collect and interpret networking logs to troubleshoot issues (for example, VPC flow logs, ELB access logs, AWS WAF web ACL logs, CloudFront logs, container logs).
- Skill 5.3.3: Identify and remediate CloudFront caching issues.
- Skill 5.3.4: Identify and troubleshoot hybrid connectivity issues and private connectivity issues.
- Skill 5.3.5: Configure and analyze CloudWatch network monitoring services.

Appendix A

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 Athena
- Amazon Data Firehose

Application Integration:

- Amazon EventBridge
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Queue Service (Amazon SQS)
- AWS Step Functions

Business Applications:

- Amazon Simple Email Service (Amazon SES)

Cloud Financial Management:

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

Compute:

- Amazon EC2
- Amazon EC2 Image Builder
- AWS Lambda

Containers:

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

Database:

- Amazon Aurora
- Amazon Aurora Serverless v2
- Amazon DynamoDB
- Amazon DynamoDB Accelerator (DAX)
- Amazon ElastiCache
- Amazon RDS
- Amazon RDS Proxy

Developer Tools:

- AWS X-Ray

Management and Governance:

- AWS Auto Scaling
- AWS Cloud Development Kit (AWS CDK)
- AWS CloudFormation
- AWS CloudTrail
- Amazon CloudWatch
- AWS Compute Optimizer
- AWS Config
- AWS Control Tower
- Amazon Managed Grafana
- AWS Managed Service for Prometheus
- AWS Organizations
- AWS Resource Access Manager (AWS RAM)
- AWS Service Catalog
- Service control policies (SCPs)
- AWS Systems Manager
- AWS Trusted Advisor
- Amazon VPC IP Address Manager (IPAM)

Migration and Transfer:

- AWS DataSync

Network and Content Delivery:

- Amazon Application Recovery Controller
- AWS Client VPN
- Amazon CloudFront
- Elastic IP addresses
- AWS Global Accelerator
- AWS PrivateLink
- Amazon Route 53
- Amazon Route 53 Resolver DNS Firewall
- AWS Site-to-Site VPN
- AWS Transit Gateway
- Amazon VPC
- VPC Endpoints
- VPC Flow Logs
- VPC peering
- VPC Reachability Analyzer

Security, Identity, and Compliance:

- AWS Certificate Manager (ACM)
- Amazon EC2 security groups
- Egress-only internet gateways
- Elastic Load Balancing (ELB)
- Amazon GuardDuty
- AWS IAM Access Analyzer
- AWS IAM Identity Center
- AWS Identity and Access Management (IAM)
- Amazon Inspector
- Internet gateways
- AWS Key Management Service (AWS KMS)
- Amazon Macie
- AWS Network Firewall
- NAT gateways
- Network ACLs
- 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
- 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:

- AWS Clean Rooms
- AWS Data Exchange
- Amazon EMR
- Amazon FinSpace
- Amazon Managed Streaming for Apache Kafka (Amazon MSK)

Application Integration:

- Amazon AppFlow
- Amazon Managed Workflows for Apache Airflow (Amazon MWAA)
- Amazon Simple Workflow Service (Amazon SWF)

Blockchain:

- Amazon Managed Blockchain (AMB)

Business Applications:

- AWS AppFabric
- Amazon Chime
- Amazon Connect
- AWS End User Messaging SMS
- Amazon One Enterprise
- Amazon Pinpoint
- AWS Supply Chain
- Amazon WorkDocs
- Amazon WorkMail

Compute:

- Amazon Lightsail
- AWS Nitro Enclaves
- AWS Parallel Computing Service
- AWS SimSpace Weaver

Database:

- Amazon Neptune
- Amazon Timestream

Developer Tools:

- AWS AppConfig
- AWS App Studio
- Amazon Q Developer

End User Computing:

- Amazon AppStream 2.0
- Amazon WorkSpaces

Frontend Web and Mobile:

- AWS AppSync
- AWS Device Farm
- Amazon Location Service

Machine Learning:

- Amazon Augmented AI (Amazon A2I)
- Amazon CodeGuru
- Amazon Comprehend
- AWS Deep Learning AMIs (DLAMI)
- AWS HealthLake
- AWS HealthOmics
- Amazon Kendra
- Amazon Lex
- Amazon Polly
- Amazon Rekognition
- Amazon Textract
- Amazon Transcribe
- Amazon Translate

Migration and Transfer:

- AWS Application Discovery Service
- AWS Application Migration Service
- AWS Migration Hub
- AWS Transfer Family

Network and Content Delivery:

- AWS App Mesh
- AWS Cloud WAN

Security, Identity, and Compliance:

- AWS CloudHSM
- AWS Payment Cryptography
- Amazon Security Lake
- AWS Signer

Storage:

- Amazon Cloud Directory
- Amazon FSx for OpenZFS

Appendix B: Comparison of SOA-C02 and SOA- C03

Side-by-side comparison

The following table shows the domains and the percentage of scored questions in each domain for the SOA-C02 exam (in use until September 29, 2025) and the SOA-C03 exam (in use beginning September 30, 2025).

SOA-C02 Domain	SOA-C03 Domain
Domain 1: Monitoring, Logging, and Remediation (20%)	Domain 1: Monitoring, Logging, Analysis, Remediation, and Performance Optimization (22%)
Domain 2: Reliability and Business Continuity (16%)	Domain 2: Reliability and Business Continuity (22%)
Domain 3: Deployment, Provisioning, and Automation (18%)	Domain 3: Deployment, Provisioning, and Automation (22%)
Domain 4: Security and Compliance (16%)	Domain 4: Security and Compliance (16%)
Domain 5: Networking and Content Delivery (18%)	Domain 5: Networking and Content Delivery (18%)
Domain 6: Cost and Performance Optimization (12%)	

Additions of content for SOA-C03

In Task1.1, the following content was added:

- Configure and manage the CloudWatch agent to collect metrics and logs from EC2 instances, Amazon Elastic Container Service (Amazon ECS) clusters, or Amazon Elastic Kubernetes Service (Amazon EKS) clusters.

In Task 3.1, the following content was added:

- Create and manage stacks of resources by using CloudFormation and the AWS Cloud Development Kit (AWS CDK).

In Task 4.1, the following content was added:

- Enforce compliance requirements (for example, Region and service selections).

In Task 5.3, the following content was added:

- Configure and analyze CloudWatch network monitoring services.

Deletions of content for SOA-C03

In Task 5.2, the following content was removed:

- Configure S3 static website hosting.

Recategorizations of content for SOA-C03

In Task 4.2, VPNs were moved to Task 5.1.

Tasks 6.1 and 6.2 in SOA-C02 were moved to Task 1.3 in SOA-C03.

Survey

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