Updated on 02/06/2026

Register

AWS Security Specialty Certification Training

3 days (21 hours)

Overview

AWS Certified Security – Specialty is an advanced certification focused on the security of AWS environments.

It validates the ability to design, deploy, and operate secure architectures, mastering identity management, encryption, network security, threat detection, and incident response.

Our training will enable you to master cloud security best practices and related AWS services: multi-account governance, access control with IAM, key management via AWS KMS, VPC network hardening, application protection with AWS WAF, and detection and investigation with GuardDuty, CloudTrail, and AWS Config.

You will learn how to reduce the attack surface, protect sensitive data, and industrialize security on AWS through organizational safeguards, isolation strategies, and observability and audit mechanisms tailored to enterprise environments.

Upon completion of the training, you will be able to secure AWS accounts at scale, implement a robust encryption strategy, implement defense in depth, and effectively prepare for the SCS-C02 exam.

Like all our training courses, this one is based on the latest AWS SCS-C02 certification framework and focuses on a practical and operational approach.

Objectives

- Understand the AWS shared responsibility model and governance requirements.
- Implement robust access control with IAM and least privilege principles.
- Protect data through encryption and key management with AWS KMS.
- Secure the AWS network with VPC, Security Groups, NACL, and private access.

- Detect, investigate, and audit with CloudTrail, AWS Config, and GuardDuty.
- Effectively prepare for SCS-C02 certification.

Target audience

- Cloud/DevOps engineers operating AWS environments
- Security engineers/DevSecOps engineers responsible for cloud security
- Cloud architects/security architects
- AWS administrators responsible for compliance, auditing, and access

Prerequisites

- Good knowledge of AWS fundamentals
- Basic security concepts
- Practical experience operating a cloud environment recommended

AWS Certified Security – Specialty (SCS-C02) Certification Training Program

[Day 1 - Morning]

Shared responsibility and governance

- Understanding the AWS shared responsibility model and its operational impacts
- Apply cloud security principles and reference pillars
- Overview of compliance requirements: ISO, SOC, PCI-DSS
- Establishing a secure organization: governance, separation of environments
- AWS Well-Architected Framework: Focus on Security Pillar
- Hands-on workshop: Analyzing an AWS architecture.

[Day 1 - Afternoon]

Identity and access management

- IAM foundations: users, groups, roles, policies, and evaluation logic
- Apply least privilege and separation of duties
- Use IAM Access Analyzer to detect external access
- Implement federation: SSO, identity providers, sessions
- Manage credentials: rotation, MFA, root account best practices
- Hands-on workshop: Create secure IAM roles.

Account and organization security

- Structure a multi-account environment with AWS Organizations
- Applying safeguards with SCPs (Service Control Policies)
- Securing the root account: MFA, restrictions, recovery procedures
- Centralize governance: administration delegation, log separation
- Implement a multi-account audit and compliance strategy
- Hands-on workshop: Deploy an organization and apply security SCPs.

[Day 2 - Morning]

Encryption and key management

- Understanding encryption at rest and in transit in AWS
- Mastering AWS KMS: keys, policies, grants, and integrations
- Distinguishing between AWS Managed Keys and Customer Managed Keys
- Implement key rotation, separation of duties, and key governance
- Applying encryption best practices on S3, EBS, and RDS
- Hands-on workshop: Encrypting S3 and RDS with KMS.

[Day 2 - Afternoon] AWS

network security

- Isolating with VPC: public/private subnets, routing, NAT, and bastion
- Control traffic with Security Groups and NACL
- Private access to services: VPC Endpoints and PrivateLink
- Architecture best practices: segmentation, micro-segmentation, "deny by default"
- Zero Trust approach and network hardening principles
- Hands-on workshop: Securing an AWS application through network segmentation and private endpoints.

Threat protection

- Application protection: AWS WAF (rules, managed rules, rate limiting)
- DDoS protection: AWS Shield and resilience strategies
- Detection: GuardDuty (signals, findings, severity, best practices)
- Responding: alerting integration, triage workflows, notifications
- SOC integration: centralization, correlation, and prioritization of alerts
- Hands-on workshop: Trigger/observe a GuardDuty finding and define a response.

[Day 3 - Morning]

Logs, auditing, and observability

- Logging with CloudTrail: events, data events, organization trails
- Compliance and drift: AWS Config (rules, aggregators, remediation)

- Centralizing logs: dedicated accounts, multi-account collection, retention
- Setting up alerts and investigations: search, filters, correlation
- Forensics: evidence collection, traceability, investigation preparation
- Hands-on workshop: Building a multi-account audit database.

[Day 3 - Afternoon]

Incident response and remediation

- Structure incident response: detection, containment, eradication, recovery
- Automating actions: Lambda, events, integrations, and approvals
- Defining playbooks: roles, responsibilities, procedures, and escalation
- Remediation: isolation, key rotation, access blocking, hardening
- Post-mortem: lessons learned, continuous improvement, prevention
- Hands-on workshop: Automate a response to a simulated incident.

Preparation for SCS-C02 certification

- Understanding the structure and expectations of the SCS-C02 exam
- Review typical scenarios: IAM, encryption, network, detection, response
- Identify common pitfalls: "best answer," costs, default security
- Resolution strategy: reading, elimination, time management
- Review checklist: critical points and priorities
- Practical workshop: Mock exam + correction.

Companies concerned

This training is aimed at both individuals and companies, large or small, wishing to train their teams in new advanced IT technology or to acquire specific professional knowledge or modern methods.

Positioning at the start of training

The positioning at the start of the training complies with Qualiopi quality criteria. Upon final registration, the learner receives a self-assessment questionnaire that allows us to assess their estimated level of proficiency in different types of technologies, as well as their expectations and personal objectives for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could be problematic for the monitoring and smooth running of the training session.

Teaching methods

Practical training: 60% practical, 40% theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and reflection sessions, and group work.

Validation

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been correctly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training course.