

SCS-C02: AWS Security – Specialty

Secure AWS workloads end to end — detection, response, identity and data protection — and prepare for the AWS Security Specialty exam.

DURATION

3 days · 24 hours

LEVEL

Advanced

CURRICULUM

9 modules · 7 labs

DELIVERYLive online, Onsite,
Corporate

Course overview

Security on AWS is a shared job, and the customer's side of that responsibility grows with every account, service and team added. Security engineers need to know how to see what is happening, respond when something goes wrong and design controls that prevent the same issue from happening again. This three-day course builds those skills with a strong practical focus.

Day one covers threat detection, incident response and logging: GuardDuty, Security Hub, Detective and Inspector, CloudTrail and centralised log architecture, and a structured incident response process for compromised credentials and instances. Day two addresses infrastructure security and identity: edge protection with WAF and Shield, network controls inside the VPC, hardening compute, and advanced IAM including policy evaluation logic, permission boundaries and cross-account access.

Day three focuses on data protection and governance. You will design encryption with KMS, including key policies and grants, manage certificates and secrets, protect S3 data with Macie and object locking, and apply governance at scale with Organizations, Control Tower and AWS Config. Labs include investigating a simulated compromise, tightening an over-permissive policy and building an encrypted, audited data store.

The final session reviews exam technique and practice scenarios. This course is aligned to the AWS Certified Security – Specialty exam and prepares you for it. AWS has been updating this exam, so confirm the current version and exam guide on the AWS Certification site before booking; we update the course to match the current outline.

Highlights

- 24 hours of advanced, security-focused training
- Hands-on threat detection and incident response
- IAM, KMS and data protection in depth
- Mapped to the AWS Security Specialty exam domains
- Scenario practice with detailed explanations

What's included

- Simulated incident investigation and containment
- IAM policy evaluation deep dive
- KMS key policies, grants and multi-Region keys
- Edge and network protection labs
- Governance at scale with Organizations and Config
- Scenario-based practice questions
- Course completion certificate from Ace Skills Consulting

Who this course is for

Who should attend

- Cloud security engineers and architects
- Security operations analysts working with AWS
- Solutions architects responsible for security design
- DevSecOps engineers

Prerequisites

- Associate-level AWS knowledge or equivalent hands-on experience
- Understanding of security fundamentals such as encryption, identity and network security
- Experience reading JSON policy documents

Detailed curriculum — 3 days, 24 hours, 9 modules, 7 hands-on labs

Day 1 Threat Detection, Incident Response & Logging

8 hours

1.1 Threat detection services

- Amazon GuardDuty findings
- Amazon Detective investigations
- AWS Security Hub and standards
- Amazon Inspector vulnerability scanning

LAB Enable detection services across accounts and triage findings · 45 min

1.2 Incident response

- Incident response planning on AWS
- Isolating and capturing evidence from EC2
- Compromised credentials and access key response
- Automating response with EventBridge and Lambda

LAB Investigate and contain a simulated instance compromise · 60 min

1.3 Logging and monitoring

- CloudTrail organisation trails
- Centralised log archive design
- VPC Flow Logs and DNS query logs
- Querying logs with Athena

LAB Query CloudTrail logs with Athena to trace suspicious activity · 35 min

Day 2 Infrastructure Security and Identity & Access Management

8 hours

2.1 Edge and network security

- AWS WAF rules and managed rule groups
- Security groups, NACLs and Network Firewall
- AWS Shield Advanced
- VPC endpoints and endpoint policies

LAB Deploy AWS Network Firewall in an inspection VPC · 50 min

2.2 Compute hardening

- Systems Manager Session Manager instead of SSH
- Container image scanning
- Patch compliance
- Instance metadata protection (IMDSv2)

2.3 Advanced IAM

- Policy evaluation logic
- Resource-based and cross-account policies
- IAM Access Analyzer
- Permission boundaries and SCPs
- ABAC with tags

LAB Tighten an over-permissive policy with Access Analyzer · 40 min

Day 3 Data Protection, Governance & Exam Readiness

8 hours

3.1 Encryption and key management

- KMS key types, key policies and grants
- Multi-Region keys and CloudHSM
- Secrets Manager rotation
- Envelope encryption
- Certificates with ACM

LAB Build an encrypted, audited data store with KMS and S3 Object Lock · 50 min

3.2 Data protection services

- Amazon Macie for sensitive data discovery
- Backup protection and vault lock
- S3 Block Public Access and access points

3.3 Governance and exam readiness

- Organizations, Control Tower and delegated administration
- Audit Manager overview
- AWS Config conformance packs
- Timed practice set with review

LAB Apply a security conformance pack with AWS Config · 30 min

Skills and tools

Skills you will build

Amazon GuardDuty

AWS Security Hub

Incident response

AWS CloudTrail

AWS WAF

AWS Network Firewall

IAM policy design

AWS KMS

Secrets Manager

Amazon Macie

AWS Config

Security governance

Tools used in class

AWS Management Console

AWS CLI

Amazon Athena

IAM Policy Simulator

IAM Access Analyzer

AWS Systems Manager

Certification exam

This course is aligned to the exam below and prepares you for it. The exam itself is booked and taken with the vendor.

Exam	AWS Certified Security – Specialty
Exam code	SCS-C02
Delivery	Online proctored, Test centre

Exam skill areas covered

Exam details are pending verification. Confirm the current exam code, format and fee on the official vendor page before booking.

Frequently asked questions

Which version of the Security Specialty exam does this cover?

The course is mapped to the current exam guide. AWS has been revising this exam, so check the AWS Certification site for the active version before booking; we update the course when the outline changes.

Do I need an associate certification first?

It is not mandatory, but associate-level knowledge and some hands-on security work on AWS make the course far more productive.

Is the course useful for SOC analysts?

Yes. The detection and incident response day is especially relevant for analysts who investigate AWS alerts.

How much hands-on work is there?

Every day includes labs, including a simulated compromise that you investigate and contain.

Can you run this for our security team?

Yes. Private batches can align exercises with your detection tools and incident response playbooks.

Book a batch or talk to an advisor

Course page: aceskillsconsulting.com/course/scs-c02-aws-security-specialty · Email: info@aceskillsconsulting.com

Chennai office

Guindy, Chennai, Tamil Nadu

Delhi office

B-95, Old Post Office Street, Shakarpur
New Delhi 110092
Office: 98180 12523

Amazon Web Services, AWS and the related marks are trademarks of Amazon.com, Inc. or its affiliates. All product names, logos, brands, trademarks and registered trademarks are the property of their respective owners. Ace Skills Consulting is an independent training provider; unless explicitly stated, it is not affiliated with, endorsed by or sponsored by any vendor mentioned on this site. Exam details are provided for guidance and may change — always confirm on the vendor's official website. Curriculum generated on 23 Oct 2026; topics and order may be adjusted by the trainer to suit each batch.