OpenCertif
Centre de formation et de certification professionnelle

SYLLABUS OFFICIEL

Examen SCS Specialty

AWS Security Specialty (SCS-C02)

Certification : AWS Certified Security — Specialty (SCS-C02)

Niveau : Specialty | Public : Security engineers cloud / Security architects / DevSecOps seniors

1. Présentation de la certification

L'examen **AWS Certified Security — Specialty (SCS-C02)** valide les compétences avancées en **sécurité cloud sur AWS** : **threat detection**, **security logging**, **infrastructure security**, **IAM**, **data protection**, et **governance / compliance**. C'est l'examen de référence pour les security engineers, security architects, et profils DevSecOps sur AWS.

L'examen exige une **maitrise approfondie** de tous les services de sécurité AWS (IAM, KMS, GuardDuty, Security Hub, Macie, Inspector, WAF, Shield) couplée à une **compréhension solide** des principes de sécurité (defense in depth, least privilege, encryption). Prérequis fortement recommandé : SAA-C03 + 2 ans d'expérience sécurité cloud. Note : **OpenCertif est Pearson VUE Authorized Test Center**.

Informations clés

Code de l'examen	**SCS-C02**
Intitulé officiel	AWS Certified Security — Specialty (SCS-C02)
Certification obtenue	AWS Certified Security Specialty
Niveau AWS	**Specialty** (expertise sécurité cloud avancée)
Éditeur officiel	Amazon Web Services (AWS)
Centre de test	**Pearson VUE** (test center ou OnVUE online proctored) ou **PSI** — OpenCertif est Pearson VUE Authorized Test Center
Format de l'examen	QCM (Multiple Choice) + Multiple Response + occasionnellement Ordering / Matching / Case Study
Langue de l'examen	Anglais (autres langues selon disponibilité : japonais, coréen, espagnol, etc.)
Validité de la certification	**3 ans**
Recertification	Repasser l'examen ou avancer au tier supérieur (Associate → Professional)
Politique de reprise	Délai d'attente de 14 jours après un échec avant de pouvoir repasser
Badge numérique	Badge officiel délivré via Credly après réussite

Position dans le catalogue AWS	Programme Certification AWS structuré en 4 niveaux : Foundational, Associate, Professional, Specialty
Réservation	AWS Training & Certification Portal : aws.amazon.com / certification
Durée de l'examen	**170 minutes**
Nombre de questions	**65 questions** (55 notées + 10 unscored)
Score requis	**750 / 1000**
Tarif	**300 USD**
Niveau d'expérience recommandé	**2 à 5 ans** d'expérience dans le domaine de spécialisation
Position dans le parcours AWS	**Specialty** — expertise technique pointue sur un domaine spécifique
Recommandation	Associate ou Professional du domaine recommandé avant Specialty
Prérequis recommandé	**5 ans** d'expérience IT security dont **2 ans** AWS security
Public type	Security engineers, security architects, DevSecOps, GRC analysts
Complémentarité	Bonne combinaison avec **CISSP**, **CEH**, ou **SC-100**

2. Profil du candidat

En tant que candidat à l'examen AWS SCS Specialty, vous développez et validez des compétences en sécurité AWS avancée : threat detection, infrastructure security, IAM, data protection, governance. Vous êtes capable de :

- Mettre en œuvre la **threat detection** avec GuardDuty.
- Configurer **Security Hub** et standards : CIS, PCI-DSS, NIST.
- Utiliser **Detective** pour investigation.
- Mettre en œuvre l'**incident response** sur AWS.
- Concevoir le **logging** centralisé : CloudTrail, VPC Flow Logs, S3 access logs.
- Configurer **CloudTrail** organization trails, data events, insight events.
- Mettre en œuvre **infrastructure security** : Security Groups, NACLs, Network Firewall, WAF, Shield.
- Sécuriser les comptes AWS : **SCPs**, **Control Tower**, **Organizations**.
- Configurer **IAM avancé** : permission boundaries, ABAC, conditions.
- **Fédération d'identités** : IAM Identity Center, SAML, AD.
- Mettre en œuvre **KMS** : customer-managed keys, key policies, rotation.
- Utiliser **CloudHSM** pour FIPS 140-2 Level 3.
- Configurer **data protection** : encryption at rest et in transit.
- Mettre en œuvre **Macie** pour data classification et PII detection.
- Sécuriser **S3** : bucket policies, block public access, S3 Object Lock.
- Configurer **Secrets Manager** et rotation automatique.
- Mettre en œuvre **compliance frameworks** : PCI-DSS, HIPAA, GDPR, SOC.

L'examen évalue spécifiquement les domaines suivants :

- Threat Detection and Incident Response
- Security Logging and Monitoring
- Infrastructure Security
- Identity and Access Management (IAM)
- Data Protection
- Management and Security Governance

3. Prérequis et public cible OpenCertif

AWS recommande les prérequis suivants pour aborder cet examen :

- **5 ans** d'expérience IT security.
- **2 ans** d'expérience hands-on AWS security.
- Connaissance des fondamentaux : **CIA Triad**, AAA, defense in depth.
- Familiarité avec les frameworks : **NIST**, **ISO 27001**, **CIS**.
- Notions de **cryptographie** : symétrique, asymétrique, hashing, PKI.
- Notions de **threat modeling**.
- **SAA-C03** ou équivalent recommandé.

- Anglais professionnel.

Public cible OpenCertif

- **Security engineers** AWS seniors.
- **Security architects** cloud.
- **DevSecOps engineers**.
- **Cloud security consultants**.
- **GRC analysts** spécialisés cloud.
- SOC engineers couvrant le cloud AWS.
- Pentesters et red teams en environnement cloud.
- Incident responders cloud.
- Profils CISSP / CEH migrant vers le cloud.
- Compliance officers et auditeurs cloud.
- Profils ayant le SAA-C03 et souhaitant approfondir la sécurité.

4. Domaines de compétences mesurées

L'examen est structuré autour de 6 grands domaines de compétences. Le tableau ci-dessous indique le poids relatif de chaque domaine dans l'évaluation finale (version 2026 — code SCS-C02). Les pondérations sont des estimations issues du guide officiel Unity / Certiport.

Domaine	Intitulé	Pondération
1	Threat Detection and Incident Response	14 %
2	Security Logging and Monitoring	18 %
3	Infrastructure Security	20 %
4	Identity and Access Management (IAM)	16 %
5	Data Protection	18 %
6	Management and Security Governance	14 %

*Remarque : l'examen UCU Programmer dure environ 50 minutes pour 40 questions, soit environ 1 minute 15 par question. La gestion du temps est essentielle. Le score requis pour valider est de **500 sur 700** (sur une échelle officielle Unity de 200 à 700 points).*

5. Détail des compétences mesurées

Cette section détaille de manière exhaustive l'ensemble des compétences couvertes par l'examen SCS Specialty, en s'appuyant sur les Objective Domains publiés par Certiport et Unity Technologies (version 2026 — code SCS-C02).

1 Threat Detection and Incident Response — 14 %

1.1 GuardDuty

- Findings types : recon, instance, account, S3, EKS, malware.
- Threat intelligence feeds.
- Custom threat lists.
- GuardDuty Malware Protection.
- Integration avec Security Hub et EventBridge.

1.2 Security Hub

- **Standards** : CIS, PCI-DSS, NIST, AWS Foundational Security Best Practices.
- Findings aggregation et insights.
- Cross-region aggregation.
- Custom actions.

1.3 Detective

- Behavior graphs.
- Investigation workflows.
- Integration avec GuardDuty.

1.4 Incident response

- **NIST** incident response phases.
- AWS incident response runbooks.
- Forensics : EBS snapshots, memory dumps.
- Isolation : security groups, NACLs.
- Automated containment avec Lambda.
- **Systems Manager Incident Manager**.

1.5 Pen testing et red teams

- AWS Customer Support Policy pour pen testing.
- Authorized services pour testing.
- Cloudgoat et autres outils.

2 Security Logging and Monitoring — 18 %

2.1 CloudTrail

- **Management events** vs **data events** vs **insight events**.
- **Organization trails**.
- Log file integrity validation.
- S3 bucket for trails avec log file lock.
- CloudTrail Lake pour query SQL.
- Athena queries sur CloudTrail.

2.2 VPC Flow Logs

- VPC, subnet, ENI level.
- S3 ou CloudWatch Logs destinations.
- Custom format avec metadata.
- Analyse avec Athena.

2.3 CloudWatch

- **Logs** : log groups, streams, retention, KMS encryption.
- **Logs Insights** queries.
- **Metrics filters** et alarms.
- Subscription filters vers Lambda, Kinesis.
- Cross-account log destination.

2.4 S3 logging

- **S3 Access Logs**.
- **CloudTrail data events** for S3.
- S3 Inventory.

2.5 Other logging

- Application Load Balancer logs.
- CloudFront access logs.
- WAF logs.
- Route 53 query logging.
- Centralized logging architecture.

3 Infrastructure Security — 20 %

3.1 Network security

- **Security Groups** : stateful rules.
- **NACLs** : stateless, numbered.
- **AWS Network Firewall** : Suricata rules.
- **WAF** v2 : Web ACLs, rules, managed rule groups, rate limiting.
- **Shield Standard et Advanced** : DDoS protection.
- **Firewall Manager**.

3.2 VPC security

- **VPC endpoints** et endpoint policies.
- **PrivateLink**.
- VPC isolation et segmentation.
- VPC Flow Logs analysis.
- VPC peering security considerations.

3.3 Compute security

- EC2 IMDSv2 enforcement.
- SSM Session Manager pour SSH-less access.
- **Patch Manager** et compliance.
- **EC2 Image Builder** pour golden AMIs.
- Bastion hosts vs SSM.

3.4 Container security

- **ECR** image scanning.
- **EKS** security : pod security, network policies, RBAC.
- **Fargate** security model.
- **Inspector** for containers.

3.5 Edge security

- **CloudFront** + WAF + Shield Advanced.
- Signed URLs, OAI, OAC.
- Field-level encryption.
- Geo restrictions.

4 Identity and Access Management (IAM) — 16 %

4.1 IAM users, groups, roles, policies

- Identity-based vs resource-based policies.
- Policy types : managed, inline, AWS managed.
- **Policy evaluation logic** : explicit deny > allow.
- **Permission boundaries**.
- Service-linked roles.
- Session policies.

4.2 Advanced IAM

- **ABAC** (Attribute-Based Access Control).
- **Tags** for access control.
- Conditions : aws:SourceIp, aws:RequestedRegion, aws:PrincipalTag.
- **NotAction** et **NotResource**.
- Cross-account access avec roles.
- STS : AssumeRole, AssumeRoleWithSAML, AssumeRoleWithWebIdentity.

4.3 IAM Identity Center

- **SSO** avec SAML 2.0, OIDC.
- Permission sets.
- Multi-account access.
- Integration avec Active Directory, Okta, Azure AD.

4.4 Identity federation

- **Cognito** User Pools et Identity Pools.
- Web identity federation : Google, Facebook, Amazon.
- Custom identity broker.

4.5 IAM Access Analyzer

- External access findings.
- Unused access findings.
- Policy generation.
- Policy validation.

5 Data Protection — 18 %

5.1 Encryption fundamentals

- **Symmetric** vs **asymmetric** encryption.
- **Envelope encryption**.
- Encryption at rest vs in transit.
- **KMS** : AWS managed, customer managed, customer provided.

5.2 KMS approfondi

- **Key policies** et grants.
- **Key rotation** : automatic, manual.
- **Multi-Region keys**.
- **Aliases** et tagging.
- Key material origin : KMS, external, CloudHSM.
- Cross-account KMS access.
- **kms:ViaService** condition.

5.3 CloudHSM

- FIPS 140-2 Level 3.
- Use cases : custom key material, third-party PKI.
- CloudHSM clusters et HA.

5.4 S3 encryption

- **SSE-S3**, **SSE-KMS**, **SSE-C**.
- Client-side encryption.
- **S3 Bucket Keys** for cost optimization.
- Default bucket encryption.
- S3 Object Lock.

5.5 Certificates et secrets

- **ACM** : public et private CA.
- **ACM Private CA**.
- Certificate rotation.
- **Secrets Manager** vs **Parameter Store**.
- Automatic rotation.

5.6 Data classification

- **Macie** : PII detection, sensitive data.
- Data classification policies.
- Findings et automation.

6 Management and Security Governance — 14 %

6.1 AWS Organizations

- **OUs** et structure.
- **SCPs** : preventive guardrails.
- Tag policies, AI services opt-out, backup policies.
- **Delegated administrator**.

6.2 Control Tower

- **Landing zones**.
- **Guardrails** : preventive et detective.
- Account Factory.
- Customizations (CfCT, AFT).

6.3 AWS Config

- **Rules** : managed et custom.
- **Conformance packs**.
- Multi-account aggregation.
- **Remediation actions**.
- Recording strategy : all resources, global resources.

6.4 Compliance frameworks

- **PCI-DSS**, **HIPAA**, **GDPR**, **SOC 2**, **ISO 27001**.
- **FedRAMP**, **HITRUST**.
- AWS shared responsibility model.
- AWS Artifact pour audit reports.

6.5 Audit Manager

- Frameworks prédéfinis.
- Custom frameworks.
- Evidence collection.
- Assessment reports.

6.6 Cost et resource governance

- **Resource Access Manager (RAM)**.
- Tagging strategies.
- Service quotas.

6. Modalités pédagogiques OpenCertif

OpenCertif accompagne les candidats au SCS Specialty à travers un parcours blended-learning complet, combinant ressources e-learning interactives, projets pratiques en IAM, KMS, CloudHSM, GuardDuty, Security Hub, Inspector, Macie, WAF, Shield, CloudTrail et incident response et accompagnement tutoré.

Format de la formation

Durée recommandée	**120 à 200 heures de préparation** recommandées. OpenCertif structure ce parcours sur 70 à 90 heures de formation tutorée avancée en sécurité cloud complétées par 80 à 120 heures de pratique hands-on et examens blancs
Modalité	100 % distanciel asynchrone, ou blended (distanciel + classes virtuelles)
Support pédagogique	Unity Certified User Courseware officiel (GMetrix) + ressources OpenCertif (modules Rise 360, scénarios immersifs)
Plateforme LMS	lmsopencertif.fr (Moodle) — accès 24/7 pendant 12 mois
Encadrement	Tutorat asynchrone par expert Unity certifié + classes virtuelles bimensuelles
Pratique requise	Au moins 150 heures de pratique Unity (recommandation officielle Unity Technologies)
Évaluations	Quiz formatifs par module, 3 projets pratiques Unity, examens blancs CertPREP
Certification finale	Passage de l’examen SCS Specialty en centre OpenCertif (CATC Certiport)

Parcours d’apprentissage proposé

- **Module 1 :** GuardDuty et threat detection.
- **Module 2 :** Security Hub et standards CIS / PCI / NIST.
- **Module 3 :** Detective et investigation.
- **Module 4 :** Incident response et forensics.
- **Module 5 :** CloudTrail : management, data, insight events.
- **Module 6 :** CloudTrail Lake et Athena queries.
- **Module 7 :** VPC Flow Logs analysis.
- **Module 8 :** CloudWatch Logs avancé et metrics filters.

- **Module 9 :** Centralized logging architecture.
- **Module 10 :** Security Groups, NACLs, Network Firewall.
- **Module 11 :** WAF v2 et Shield Advanced.
- **Module 12 :** Firewall Manager.
- **Module 13 :** VPC endpoints et PrivateLink security.
- **Module 14 :** EC2 IMDSv2 et SSM Session Manager.
- **Module 15 :** Container security : ECR, EKS, Fargate.
- **Module 16 :** IAM policies avancées et evaluation logic.
- **Module 17 :** ABAC, conditions, permission boundaries.
- **Module 18 :** IAM Identity Center et federation.
- **Module 19 :** Cognito User Pools et Identity Pools.
- **Module 20 :** IAM Access Analyzer.
- **Module 21 :** KMS approfondi : keys, policies, rotation.
- **Module 22 :** CloudHSM et FIPS 140-2.
- **Module 23 :** S3 encryption : SSE-S3, SSE-KMS, SSE-C.
- **Module 24 :** ACM, Private CA, Secrets Manager.
- **Module 25 :** Macie et data classification.
- **Module 26 :** Organizations et SCPs.
- **Module 27 :** Control Tower et guardrails.
- **Module 28 :** Config rules et conformance packs.
- **Module 29 :** Compliance frameworks : PCI, HIPAA, GDPR.
- **Module 30 :** Audit Manager.
- **Module 31 :** Examens blancs Tutorials Dojo / Stephane Maarek.

7. Ressources d’étude officielles

En complément du parcours OpenCertif, les ressources officielles Unity Technologies et Certiport suivantes sont fortement recommandées :

- Page officielle AWS Certification : **aws.amazon.com / certification**.
- Page officielle OpenCertif : opencertif.fr / aws.
- **AWS Skill Builder** : skillbuilder.aws (cours officiels gratuits et payants).
- **AWS Cloud Quest** : jeu d’apprentissage cloud gamifié.
- Exam Prep officiels sur Skill Builder.
- **AWS Whitepapers** et **FAQs** par service.
- **AWS Well-Architected Framework** documentation.
- Chaîne YouTube officielle AWS et AWS re:Invent.
- **Stephane Maarek**, **Adrian Cantrill** (Udemy / cours réputés).
- **Tutorials Dojo** et **WhizLabs** : examens blancs.
- **AWS Certified Cloud Practitioner** et autres Cert Guides (Ben Piper, McGraw Hill).
- Communauté : **AWS re:Post** (anciennement Stack Overflow AWS).
- Badge officiel délivré via **Credly**.
- **Stephane Maarek SCS-C02 Udemy course**.
- **Tutorials Dojo SCS-C02 Practice Exams** (Jon Bonso).
- **Adrian Cantrill SCS-C02 course**.
- **AWS Security Blog** : aws.amazon.com/blogs/security.
- **AWS Security Specialty Official Study Guide**.
- Page officielle SCS-C02 : aws.amazon.com / certification / certified-security-specialty.
- AWS re:Inforce conference videos et talks.

8. Modalités de passage de l’examen

Inscription	Via OpenCertif ou directement auprès d’un centre Certiport
Centre d’examen	OpenCertif — Centre Certiport Authorized Testing Center (CATC) / Pearson VUE
Mode de passage	En centre uniquement (Unity n’autorise pas l’examen OnVUE à distance pour les certifications UCU — présence sur site requise)
Pièce d’identité	1 pièce d’identité avec photo obligatoire le jour de l’examen (pour les mineurs : autorisation parentale et CNI / passeport)

Aménagements	Demande possible auprès de Certiport (temps additionnel, assistance technique)
Résultat	Score communiqué immédiatement à la fin de l’examen (échelle 200-700, seuil de réussite 500)
Validité de la certification	3 ans à partir de la date de réussite — attribuée une seule fois (stackable, pas de renouvellement payant requis)
Politique de reprise	Délai d’attente de 24 heures avant la 1re reprise. Voucher retake à utiliser sous 60 jours après l’échec.
Badge numérique	Badge officiel délivré via Credly et intégrable à LinkedIn, CV, portfolio, sites de recrutement

9. Contact et inscription

Pour toute information complémentaire, demande de devis ou inscription à la formation préparatoire au SCS Specialty, l'équipe OpenCertif reste à votre disposition. OpenCertif est un Centre Certiport Authorized Testing Center (CATC) habilité à délivrer les certifications Unity Certified User.

OpenCertif
Centre de formation et de certification

app.opencertif.fr
lmsopencertif.fr

Centre agréé Certiport / Pearson VUE
Certifié Qualiopi — Actions de formation

10. Mentions légales et version

Ce syllabus est établi par OpenCertif sur la base des Objective Domains officiels publiés par Certiport pour la certification SCS Specialty, dans sa version applicable (version 2026 — code SCS-C02). Les compétences mesurées, les pondérations et les objectifs présentés reflètent fidèlement la structure de l'examen telle que publiée par Unity Technologies via Certiport.

Version du syllabus : 2026.05 — Édition mai 2026
Source officielle Certiport : certiport.pearsonvue.com/Certifications/Unity/Certified-User/Certify
Source officielle Unity : unity.com/products/unity-certifications/user-programmer
Page OpenCertif : opencertif.fr/unity-user-programmer