AWS Certified Security – Specialty (SCS-C02)

Quick Exam Refresher

*This is your condensed, high-impact review guide for the **AWS Certified Security – Specialty** exam. Use it just before test time — not for deep study. It's structured to help you recall the most tested services, configurations and security best practices.*

Security Specialty (SCS-C02) Domains

Focus on infrastructure protection, identity verification and logging:

- **Domain 1:** Threat Detection and Incident Response – 14%
- **Domain 2:** Security Logging and Monitoring – 18%
- **Domain 3:** Infrastructure Security – 20%
- **Domain 4:** Identity and Access Management – 16%
- **Domain 5:** Data Protection – 18%
- **Domain 6:** Management and Security Governance – 14%

Quick Reminder: How the Exam Works

- **Number of Questions:** 65 (50 scored + 15 unscored)
- **Format:** Multiple choice + multiple response
- **Time Limit:** 170 minutes
- **Passing Score:** 750/1000
- **Test Provider:** Pearson VUE (online or onsite)

Remember — You Don't Need to Be Perfect to Pass

The passing score is **750/1000**, meaning you can miss around **10–15 scored questions** and still pass. Expect real-world scenarios, especially around IAM misconfigurations, S3 data exposure, GuardDuty alerts, and compliance remediation.

Domain 1: Threat Detection and Incident Response (14%)

Core Concepts:

- **Incident Response Lifecycle:** Preparation, Detection, Containment, Eradication, Recovery, Post-Incident.
- **Credential Compromise:** Use IAM to delete access keys, rotate credentials. Apply SCPs to restrict access.
- **Isolating Resources:** Use quarantine VPCs, Security Groups, stop instance, remove IAM permissions. Use SSM Session Manager (no SSH needed).

Key Services:

- **GuardDuty:** Detects threats using VPC Flow Logs, CloudTrail, DNS. Alerts like crypto-mining, port scans.
- **Macie:** Finds PII in S3, alerts on large downloads or public exposure.
- **Inspector:** Scans EC2 and ECR for CVEs and config risks.
- **Detective:** Investigate GuardDuty findings with correlated logs and flow data.
- **Security Hub:** Aggregates findings from GuardDuty, Macie, Inspector. Central view. Uses AWS Security Finding Format (ASFF).

Response Tools:

- **EventBridge + Lambda:** Automate responses to findings (e.g., auto-isolate EC2).
- **Snapshot + Forensics:** Use EBS snapshots and VPC Traffic Mirroring for investigation.
- **CloudTrail & Athena:** Review logs, queries to find API misuse.
- **Access Analyzer:** Identifies public or cross-account access risks.

Domain 2: Security Logging and Monitoring (18%)

Core Concepts:

- **Full Visibility:** Turn on logs for all services. Enable organization-wide trails.
- **Alerting:** Use CloudWatch Logs Metric Filters + Alarms.
- **Log Centralization:** Send all logs to central S3. Use KMS for encryption.

Key Services:

- **CloudTrail:** Tracks API calls. Enable org trail, multi-region. Data events for S3/Lambda. Validate logs.
- **CloudWatch Logs/Alarms:** Monitor logs. Filter for "Unauthorized" or "ConsoleLogin".
- **VPC Flow Logs:** Network metadata per ENI. Accept/Reject traffic visibility.
- **Route 53 Resolver Logs:** Captures DNS queries. Detect DNS exfiltration.
- **Config:** Monitors config changes. Use managed rules. Aggregator for all accounts.

Analysis Tools:

- **Athena:** Query logs in S3 with SQL.
- **CloudWatch Logs Insights:** Real-time log search tool.
- **Security Hub Insights:** Shows compliance score, top findings.

Troubleshooting Tips:

- CloudTrail not delivering? Check S3 bucket policy, KMS permissions.
- Logs missing? Check delivery IAM role, retention, region coverage.
- Alarm not firing? Check thresholds, metric filter patterns.

Domain 3: Infrastructure Security (20%)

Core Concepts:

- **Defense in Depth:** Use WAF, Shield, SG, NACL, NFW together.
- **Network Isolation:** Private subnets, no public IP, NAT for egress.
- **Edge Security:** Filter at CloudFront/WAF/ALB before VPC.

Key Services:

- **Security Groups:** Stateful. Restrict by IP or SG.
- **NACLs:** Stateless. Deny/Allow by port/IP.
- **VPC Endpoints:** Private access to AWS services. Block S3 to only allow via endpoint.
- **Transit Gateway:** Connect VPCs/accounts at scale.
- **AWS Network Firewall:** Deep packet inspection. Egress control.
- **WAF:** L7 filtering. Rate limiting. OWASP protections.
- **Shield Advanced:** DDoS protection, DRT access.

Compute Security:

- **EC2:** Use hardened AMIs. Disable SSH, use SSM. Patch with SSM Patch Manager.
- **Inspector:** Detects OS CVEs. Scans EC2, ECR.
- **IAM Roles:** Attach to EC2/Lambda. Never hardcode keys.
- **EKS IRSA:** Use IAM roles per pod via OIDC.

Monitoring:

- **VPC Reachability Analyzer:** Troubleshoot connectivity.
- **Traffic Mirroring:** Deep inspection of packets.

Domain 4: Identity and Access Management (16%)

Core Concepts:

- **Least Privilege:** Minimal access. Use roles not users.
- **Federation:** Use IAM Identity Center or SAML/OIDC.
- **Session Controls:** Use session policies, permission boundaries.

Key Services:

- **IAM:** Users, Groups, Roles. Inline vs Managed policies.
- **STS:** AssumeRole, temporary credentials. Used in federation.
- **IAM Identity Center (SSO):** Manage access across accounts.
- **Access Analyzer:** Detect public/cross-account access.
- **Credential Reports:** Audit keys, password, MFA status.
- **Policy Simulator:** Test access issues.

Policy Types:

- **Identity Policy:** Attached to users/roles. Needs explicit Allow.
- **Resource Policy:** On S3, KMS, etc. Has Principal.
- **SCP:** Org-level control. Applies even to root.
- **Permission Boundaries:** Limit max permissions a role/user can get.

Troubleshooting:

- Access Denied? Check identity policy, resource policy, SCP, boundary.
- MFA required? Use aws:MultiFactorAuthPresent condition.

Domain 5: Data Protection (18%)

Core Concepts:

- **Encrypt Everything:** At rest and in transit. KMS central to encryption.
- **Key Management:** Know KMS key types, policies, grants, rotation.
- **Data Lifecycle:** Enforce retention, deletion, WORM where needed.

Key Services:

- **KMS:** Envelope encryption. Customer vs AWS-managed keys. Rotation, key policy.
- **CloudHSM:** Dedicated HSM cluster. Required for FIPS-level compliance.
- **Secrets Manager:** Store/rotate secrets. KMS encrypted.
- **SSM Parameter Store:** Simpler alternative for secrets.

Encryption at Rest:

- **S3:** SSE-S3, SSE-KMS, SSE-C. Enforce with bucket policy.
- **EBS:** Volume-level encryption. Default setting. KMS key.
- **RDS:** Encrypt at launch. TDE for Oracle/SQL Server.
- **EFS:** Encrypt at rest and in transit. KMS integration.

Encryption in Transit:

- TLS/SSL everywhere. Use ACM certs for ALB, CF.
- Use VPN over Direct Connect if MACsec not supported.
- S3 bucket policy can enforce SecureTransport.

Data Integrity:

- **S3 Object Lock:** WORM. Use for compliance.
- **CloudTrail log validation:** Prevent tampering.

Domain 6: Management and Security Governance (14%)

Core Concepts:

- **Multi-Account Strategy:** Use AWS Organizations for isolation, governance.
- **Centralized Management:** Delegate Security Hub, GuardDuty admin.
- **Compliance Automation:** Use Config, Security Hub, Audit Manager.

Key Services:

- **AWS Organizations:** SCPs, tag policies, consolidated billing.
- **Control Tower:** Automates landing zones, guardrails.
- **Security Hub:** CIS, PCI checks. Org-wide aggregation.
- **Config Aggregator:** View config from all accounts.
- **Audit Manager:** Collect evidence for ISO, SOC2, etc.
- **Trusted Advisor:** Security checks (e.g., root with no MFA).

SCP Tips:

- Deny DeleteTrail to prevent disabling logging.
- Deny s3:PutBucketPolicy if public access not allowed.
- Restrict regions, services per OU.

Automation and IaC:

- Use CloudFormation with IAM role boundaries.
- Detect drift. Integrate security checks in pipelines.

Visibility and Reporting:

- Use AWS Config and Security Hub scores to track posture.
- Use Macie to identify PII.
- Use Trusted Advisor to detect exposure (public S3, unused creds).

Core AWS Services You Must Know

(High Priority – Frequently Tested)

Service	What You Must Know
IAM	Users, roles, policies, permission boundaries, trust policies, federated access
KMS	Key policies, envelope encryption, grants, rotation, CMK vs AWS-managed vs BYOK
CloudTrail	API logging, multi-region, org trails, data events, log validation
CloudWatch	Logs, metrics, alarms, metric filters, dashboards, Logs Insights, event automation
GuardDuty	Threat detection from CloudTrail, VPC Flow Logs, DNS; auto findings; centralized admin
Security Hub	Aggregates findings, CIS/FSP/PCI standards, Insights, integrates with ASFF
Macie	S3 data classification (PII), alerts on sensitive data access or public buckets
AWS Config	Resource compliance tracking, managed rules, custom rules, aggregators, remediation
Inspector	EC2 and ECR CVE scanning, network reachability, automatic assessments
Detective	Investigate GuardDuty findings with correlated CloudTrail, VPC logs, EKS audit logs
Organizations	Multi-account setup, SCPs, central billing, delegated admin setup
SSM (Systems Manager)	Session Manager for access without SSH, Patch Manager, Automation documents
S3	Encryption (SSE-S3, SSE-KMS), bucket policies, block public access, Object Lock

VPC	Security groups, NACLs, subnet types, route tables, endpoints, traffic flow
Secrets Manager	Encrypted secret storage, automatic rotation, IAM access control
ACM	TLS/SSL certs for ALB, CloudFront, etc., public/private certs
WAF	L7 protection, rate-based rules, AWS managed rules, web ACLs
Shield	DDoS protection, Shield Standard vs Advanced, DRT access
EC2	IAM roles, hardened AMIs, encrypted volumes, SSM access, Inspector scans
Athena	SQL queries on logs stored in S3 (CloudTrail, VPC, etc.)

Other AWS Services You Should Know

(Moderate Priority – Occasionally or Partially Tested)

Service	What You Must Know
CloudHSM	Dedicated HSMs for custom crypto or compliance, used with KMS custom key store
CloudFront	Edge delivery, origin access control, integrates with WAF and ACM for HTTPS
Route 53 Resolver	DNS query logging, DNS Firewall, DNS-level egress control
IAM Identity Center	Centralized SSO across accounts, permission sets, integrates with AD/SAML
STS	Temporary credentials, AssumeRole, federation (SAML, OIDC), session policies
EBS	Encryption at rest via KMS, enforced via default settings, snapshots stay encrypted
EFS	Supports KMS encryption at rest and TLS for in-transit encryption
RDS	KMS encryption, TDE for Oracle/SQL Server, public access control
DynamoDB	Always encrypted at rest, optionally with customer CMK
ElastiCache	Encryption options (in-transit and at-rest), authentication and access restrictions
Redshift	Encryption with KMS or HSM, logging and audit features
Backup	Centralized backups, Vault Lock (WORM), cross-region backup
CloudFormation	Secure deployment, IAM roles for stacks, drift detection, stack policies
CloudShell	CLI in browser for secured access without local setup
CloudTrail Lake	Advanced log querying (data lake for CloudTrail), long-term retention

Amazon EventBridge	Automate responses to findings, integrate with GuardDuty, Config, Security Hub
Trusted Advisor	Security checks: root MFA, public S3, exposed ports, credential audits
Access Analyzer	Detect public/cross-account access to IAM roles, S3, KMS, etc.
SSM Parameter Store	Encrypted parameter storage, alternative to Secrets Manager
Transit Gateway	Centralized VPC routing, attach NFW, egress filtering
AWS Firewall Manager	Policy-based WAF/Security Group enforcement across accounts
Amazon MQ/Kafka	Data protection configurations, encryption in transit and at rest
Elastic Load Balancer	TLS offload, cert via ACM, integration with WAF (for ALB only)
SCP (Service Control Policies)	Org-wide permission limits; applied even to root
Tag Policies	Enforce consistent tagging for governance and security automation
Audit Manager	Framework-based evidence collection for compliance reporting
Well-Architected Tool	Identify security risks, track improvements via Security Pillar
AWS Artifact	Access AWS compliance reports (SOC, PCI, etc.) for shared responsibility
Amazon EKS	IRSA for IAM per pod, EKS audit logs, GuardDuty EKS protection
AWS Cost Anomaly Detection	Detect billing anomalies that may indicate misuse or breach
Macie Findings + EventBridge	Automate response to sensitive data exposure