CloudNinja.pro

SPECIALTY · SCS-C03

AWS Certified Security – Specialty

SCS-C03 Cheat Sheet

CloudNinja · cloudninja.pro · Free — no signup required

Every security service in scope, every detection and response pattern, every IAM and data-protection decision the SCS-C03 exam actually tests — organised around the six exam domains. Assumes ≥ 5 years of IT security and ≥ 2 years of AWS.

EXAM SNAPSHOT

- **65 questions** — 50 scored + 15 unscored
- **170 minutes** total time
- **750 / 1000** to pass
- **$300 USD** exam fee

- **Detection** — 16%
- **Incident Response** — 14%
- **Infrastructure Security** — 18%
- **Identity & Access Management** — 20%
- **Data Protection** — 18%
- **Foundations & Governance** — 14%

FREE SCS-C03 practice exam →

Closed or retired services. Amazon CodeGuru Security reached end of support on 20 November 2025 RETIRED; use Amazon Inspector Code Security (SAST, secrets and IaC scanning of GitHub / GitLab repositories) instead. Amazon Q Developer is still on the guide, but its IDE plugins and paid subscriptions (Pro) reach end of support on 30 April 2027 and its CLI is now Kiro END OF SUPPORT · ON GUIDE. Amazon Q Business, AWS Audit Manager and CloudTrail Lake are closed to new customers but still on the SCS-C03 guide CLOSED · ON GUIDE. Systems Manager Incident Manager and Change Manager, Simple AD and the *Detect* feature of AWS IoT Device Defender are closed to new customers too DEPRECATED; Device Defender Audit stays available. Know them for the exam, but pick the replacement for a new design (list on the last page).

1 · Shared Responsibility & Governance Foundations

- **AWS** is responsible for security *of* the cloud (hardware, facilities, hypervisor, managed-service backplane).
- **You** are responsible for security *in* the cloud (IAM, patching unmanaged OS, encryption choices, network controls, app code).
- **Degree of responsibility varies by service** — more for EC2, less for DynamoDB, almost none for Lambda runtime.
- **AWS Artifact** — self-service portal for AWS compliance reports (SOC 1/2/3, PCI DSS AoC, ISO, FedRAMP, HIPAA, IRAP). Third-party organisation agreements.
- **AWS Well-Architected Tool** — Security pillar review; lenses for Financial Services, SAP, Serverless.
- **AWS Trusted Advisor** — security checks (MFA on root, IAM password policy, SG 0.0.0.0/0, S3 public, RDS public).

2 · AWS Organizations, Control Tower & Multi-Account Security

Canonical Secure Landing Zone

Account / OU	Purpose
Management	Organizations, billing, Control Tower only. Zero workloads, zero humans day-to-day. Root email + hardware MFA.
Log Archive	Central immutable log store (CloudTrail, Config, VPC flow, GuardDuty, WAF). S3 Object Lock + SSE-KMS with CMK replicated cross-Region.
Audit / Security Tooling	Delegated admin for GuardDuty, Security Hub, Config, IAM Access Analyzer, Macie, Inspector, Firewall Manager, Security Lake (Audit Manager is closed to new customers).
Networking	TGW, DX Gateway, Route 53 Resolver, Shared VPCs via RAM.
Identity	IAM Identity Center store, Directory Service for AD integration, Verified Access + Verified Permissions.
Workloads OU	Prod / staging / dev with progressively stricter SCPs.

Policy Types and Evaluation Order

- **SCPs** — Organizations-wide permission ceilings on principals. Never grant.
- **Resource Control Policies (RCPs)** — newer; Organizations-wide ceilings on resources (S3, SQS, Secrets Manager, KMS, STS). Prevents grants from outside principals.
- **Permission boundaries** — maximum permissions an identity-based policy can grant to a user/role.
- **Session policies** — passed at AssumeRole to further restrict that session.
- **Evaluation** — explicit deny always wins. Order: SCP & RCP → resource policy → identity policy → permission boundary → session policy → VPC endpoint policy.

AWS Control Tower

- Managed landing zone — bootstraps Log Archive + Audit accounts, IAM Identity Center, StackSets for baseline guardrails.
- **Preventive guardrails** — SCPs that block disabling CloudTrail, log tampering, etc.
- **Detective guardrails** — Config rules with continuous evaluation.
- Account Factory / AFT (Account Factory for Terraform) for IaC-driven provisioning.

3 · Identity & Access Management (IAM)

IAM Core

- **Principals** — root, IAM user, IAM role, federated user. **Always** use roles for services and federated users; never long-lived user keys in code.
- **Policy types** — identity-based, resource-based, permission boundary, SCP/RCP, session.
- **Policy elements** — Version, Statement, Sid, Effect, Action/NotAction, Resource/NotResource, Principal/NotPrincipal, Condition.
- **Condition keys** — `aws:PrincipalOrgID`, `aws:PrincipalTag/*`, `aws:ResourceTag/*`, `aws:SourceIp`, `aws:SourceVpce`, `aws:SecureTransport`, `aws:MultiFactorAuthPresent`, `aws:PrincipalArn`, `aws:RequestTag/*`, `kms:ViaService`, `aws:ViaAWSService`, `ec2:ResourceTag/*`.
- **ABAC** — attribute-based access control using principal + resource tags; scales beyond RBAC.
- **IAM Access Analyzer** — external access (resources exposed outside org), unused access (roles/users/keys not used for N days), custom policy checks (compare policies, check before deploy), policy generation from CloudTrail activity.
- **Access Advisor** — show service last-accessed; prune unused permissions.
- **Credentials Report** — CSV of every user + their creds ages / MFA / last use.

AWS IAM Identity Center

- Workforce SSO to all AWS accounts + external SaaS (Salesforce, Slack).
- Identity source: built-in, Active Directory (Managed AD / AD Connector), external IdP (Okta, Entra, Ping) via SAML 2.0 + SCIM 2.0.
- Permission Sets = IAM roles auto-provisioned in member accounts. Session 1–12 h.
- Trust relationships managed centrally; no long-lived creds.

AWS STS — Temporary Creds

- `AssumeRole` — cross-account + break-glass; `AssumeRoleWithSAML` / `AssumeRoleWithWebIdentity` — federated. External ID mitigates the "confused deputy" problem.
- **Regional endpoints** reduce latency + tolerate Region outages; enable per Region in account.
- **Session tags** propagate attributes into ABAC decisions downstream.

Directory Service & Cognito

- **AWS Directory Service** — Managed Microsoft AD (full MSFT AD, multi-AZ, cross-account trust, LDAPS, MFA), AD Connector (proxy to on-prem AD), Simple AD DEPRECATED (closed to new customers → Managed Microsoft AD or AD Connector).
- **Amazon Cognito** — User Pools (authentication: sign-in, MFA, hosted UI, federation via SAML/OIDC/social); Identity Pools (authorisation: exchange auth tokens for temporary AWS creds).
- **Amazon Verified Permissions** — fully-managed Cedar policy engine for application authorisation; integrates with Cognito / OIDC.

4 · Encryption, Keys & Secrets

AWS KMS

Feature	Detail
Key types	AWS-owned (free, no visibility) · AWS-managed (*aws/service*, per-service, no key policy edit) · Customer-managed (CMK, full control).
Key material	KMS-generated (default), imported (BYOK — wrapped with public wrapping key), CloudHSM-backed (custom key store).
Algorithms	Symmetric (AES-256-GCM) for encrypt/decrypt + DEKs; asymmetric (RSA, ECC) for encrypt/decrypt / sign/verify; HMAC; SM2 (China).

Feature	Detail
Multi-Region keys	Replicas in multiple Regions sharing key ID + material — decrypt ciphertext produced in any replica Region.
Key policies	Primary authorisation on the CMK. Must reference root, or grant via `kms:*` to the account. Key policy + IAM policy both evaluated.
Grants	Temporary delegated access; used by AWS services (EBS, RDS) behind the scenes.
kms:ViaService	Condition restricts key use to specific AWS service calls (e.g., only via S3).
Key rotation	Automatic annual for KMS-generated symmetric CMKs. Manual for imported/asymmetric — create new key + re-wrap DEKs.
Envelope encryption	CMK encrypts data encryption keys (DEKs); DEKs encrypt data. Minimises KMS API calls + gives ciphertext portability.

AWS CloudHSM

- Single-tenant FIPS 140-2 Level 3 HSM cluster in your VPC. You manage keys + users directly (PKCS#11, JCE, CNG/KSP).
- Required for regulated keys (root of PKI, payment HSM-equivalent, BYOK wrapping).
- Integrate as a KMS custom key store, or use directly from apps.

Certificates

- **AWS Certificate Manager (ACM)** — free public TLS certs (DNS/email validation), auto-renewed on integrated services: ALB/NLB/CloudFront/API Gateway/Elastic Beanstalk/Nitro Enclaves (and App Runner, closed to new customers).
- **AWS Private CA (AWS Private Certificate Authority)** — managed private CA hierarchy (root + subordinate). Issue X.509 for internal TLS, mTLS, IoT device identity. CRL to S3, OCSP supported.

Secrets Management

- **AWS Secrets Manager** — automatic rotation via Lambda; native rotation for RDS / Redshift / DocumentDB. Cross-account resource policy, cross-Region replication. 64 KB max.
- **SSM Parameter Store** — free (Standard, 4 KB, 40 TPS). SecureString encrypts with KMS. Advanced tier adds 8 KB, higher throughput, parameter policies (expiration, notification).
- Best practice: app identity (role) + reference secret ARN via env var or SDK call at runtime; never bake secrets into images or code.

5 · Detection — Finding Threats and Misconfiguration

Service	Detects
Amazon GuardDuty	Threat detection on CloudTrail, VPC Flow, DNS, EKS audit, S3, RDS Protection, Lambda, Runtime Monitoring (EKS / ECS on Fargate / EC2), Malware Protection for EC2 + S3. Finding severity high/medium/low.
Amazon Inspector	Continuous vulnerability scanning — EC2 (OS CVEs + network reachability), ECR container images, Lambda + Lambda layers. CVSS with EPSS + exploitability. Findings to Security Hub.
Amazon Macie	S3 data discovery — PII, credentials, regulatory data (HIPAA, PCI) via managed + custom data identifiers.
Amazon Detective	Graph-based incident investigation: GuardDuty findings, VPC Flow, CloudTrail, EKS audit. Pivot from finding to entities and timelines.
AWS Security Hub	Aggregator of findings from GuardDuty, Inspector, Macie, IAM Access Analyzer, Firewall Manager, Health, Route 53 Resolver DNS Firewall, 3rd-party via ASFF. Standards: AWS FSBP, CIS v1.4, CIS v3.0.0, PCI DSS v3.2.1, PCI DSS v4.0.1, NIST SP 800-53 Rev. 5. Delegated admin.

Service	Detects
AWS Config	Resource inventory + compliance rules + auto-remediation via SSM Automation. Aggregators for cross-account dashboards. Conformance Packs package rules + remediation.
AWS CloudTrail	Management + data events + Insights (anomaly detection). Org-level trail to Log Archive S3 with Object Lock + SSE-KMS. Integrity via digest files (log-file validation).
AWS CloudTrail Lake CLOSED · ON GUIDE	Managed event data store; SQL over the full event history (7–3653 day retention); non-AWS sources via open audit logs; federated queries. Closed to new customers since 31 May 2026 → CloudWatch, or trail logs in S3 queried with Athena.
Amazon CloudWatch	Metrics + alarms + dashboards; Logs Insights + subscription filters. Composite alarms, anomaly detection, metric math, cross-account.
Amazon OpenSearch Service	Central SIEM-style log analytics; alerting, anomaly detection, SAML SSO. Ingest via Firehose or native log subscription.
Amazon Athena	SQL over S3 (CloudTrail, VPC Flow, ALB, CloudFront, WAF, GuardDuty exports). Partitioned Parquet = cheap + fast.
Amazon Managed Grafana	Dashboards on CloudWatch, X-Ray, OpenSearch, Prometheus, Athena, Timestream.
AWS User Notifications	Central channel for AWS-originated notifications — route to Slack/Teams/email/SMS; replaces hand-rolled EventBridge→SNS→Chatbot plumbing for many use-cases.

Amazon Security Lake

- Managed security data lake: normalises logs to OCSF in Apache Parquet in S3. Ingests CloudTrail, VPC Flow, Route 53 Resolver, EKS audit, Security Hub findings, + 30+ partner sources.
- Query with Athena, Redshift, OpenSearch, third-party SIEM (Splunk, Datadog, Sumo Logic) via subscriber access.
- Org-wide; delegated admin; retention + lifecycle managed by Lake.

6 · Incident Response

Canonical Event-Driven Response

1. **Source** — GuardDuty finding / Config NON_COMPLIANT / CloudWatch alarm / CloudTrail event / Health event / Security Hub custom insight.
2. **Router** — EventBridge rule (default bus for AWS services; custom bus for application events).
3. **Action** — SSM Automation document (runbook), Lambda, Step Functions (Incident Manager response plans on older answers; closed to new customers).
4. **Notification** — SNS → Chatbot / User Notifications → Slack, Teams, email, SMS.
5. **Evidence** — OpsCenter OpsItem, Security Hub finding, Config compliance history (Incident Manager timelines and Audit Manager evidence on older answers).

Forensics on EC2

- **Automated Forensics Orchestrator for Amazon EC2** — AWS solution automating triage: isolate instance (change SG), snapshot EBS, capture memory via SSM, preserve evidence in a forensic account with chain-of-custody.
- **Manual triage**: detach from ASG (avoid termination), remove from Target Group, replace SG with quarantine (deny egress), EBS snapshot, share snapshot to forensics account, launch forensic instance with read-only volume attached.

Other Response Services

- **AWS Systems Manager Incident Manager** DEPRECATED — closed to new customers since 7 Nov 2025 (→ OpsCenter, or partner paging such as PagerDuty). On-call rotas, escalation plans, chat channel auto-populated, response plan invokes SSM Automation; timeline + postmortem.
- **AWS Fault Injection Service (FIS)** — controlled chaos (stop instances, throttle, add latency, kill pods). Stop conditions on CloudWatch alarms — use it to test that your IR fires.

- **AWS Backup** — restore-testing plans; cross-account + cross-Region copy; vault lock for ransomware-proof retention.
- **AWS Resilience Hub** — score apps against RTO/RPO targets; recommends fixes; integrates with FIS.
- **Amazon Application Recovery Controller** — routing controls + readiness checks for deterministic Region failover.

7 · Infrastructure Security — Network Controls

Control	Role
Amazon VPC	Subnet segmentation (public / private / isolated); Network ACLs (stateless); Security Groups (stateful, SG-to-SG references); VPC endpoints (private access to AWS services); Flow Logs.
Network Access Analyzer	Org-wide evaluation — "no internet egress from DB subnets", "no non-TLS ingress". Uses scopes + JSON findings.
AWS Network Firewall	Managed Suricata; stateful L3-L7 + TLS inspection; centralised in inspection VPC behind GWLB.
AWS Firewall Manager	Org-wide: WAF, Shield Advanced, SG baselines, Network Firewall, Route 53 Resolver DNS Firewall, NACL policies.
AWS WAF	L7 managed + custom rules on ALB/CloudFront/API GW/AppSync/Cognito/Verified Access/App Runner (closed). Bot Control, ATP, ACFP, Fraud Control.
AWS Shield Standard / Advanced	DDoS. Advanced adds DRT, cost protection, global threat dashboard, Route 53 / Global Accelerator integration.
AWS PrivateLink	Expose service to another VPC/account privately; consumer never touches public IPs.
AWS Verified Access	Zero-trust app access — identity + device posture per request, no VPN.
AWS Client VPN / Site-to-Site VPN / Direct Connect / Transit Gateway / Route 53	See ANS-C01 cheat sheet for deep detail; in SCS-C03 exam they appear as context for rules/attribute-based decisions.
Elastic Load Balancing	TLS termination (ACM), WAF on ALB, mTLS on ALB, SG on ALB, security policies controlling TLS versions/ciphers.
Route 53 Resolver DNS Firewall	Allow / block lists + AWS-managed threat domain feeds; block DNS tunnelling and C2.
Amazon CloudFront	Edge TLS, WAF + Shield, signed URLs/cookies, field-level encryption, OAC for S3 origin.

8 · Compute Workload Security

Amazon EC2

- **IMDSv2 required** — token-based metadata; block v1 in launch template to mitigate SSRF → creds theft. Service-linked condition: `ec2:MetadataHttpTokens = required`.
- **EC2 Instance Connect** — temporary SSH keys pushed to metadata for 60 s; no long-lived keys. IAM-gated; browser or CLI.
- **Session Manager** — shell into instances with no SSH, no bastion, no open ports. KMS-encrypted, logged to S3 + CloudWatch.
- **EC2 Image Builder** — golden-AMI pipeline with automated scanning via Inspector; distribute + sign images.
- **Nitro Enclaves** — isolated CPU/RAM with no persistent storage or networking; for PII, crypto ops, private-key handling. KMS attestation: only code running in an enclave with a specific PCR can decrypt.
- **Amazon Data Lifecycle Manager** — scheduled EBS + AMI snapshot policies + retention + cross-account copy for DR / forensics baseline.

Containers & Serverless

- **Amazon EKS** — IAM Roles for Service Accounts (IRSA) or Pod Identity for pod-level creds; admission controllers; Security Groups for Pods; audit log to CloudWatch. GuardDuty EKS Runtime Monitoring.
- **Amazon ECR** — Basic (CVE only) or Enhanced scanning via Inspector; signing via AWS Signer + notation.
- **AWS Lambda** — least-privilege execution role, env vars encrypted with KMS, VPC if reaching private resources, Inspector (Lambda code + dependency scanning) for code scanning, signing via Signer.
- **Amazon API Gateway** — IAM auth, Cognito, Lambda authorizer, mTLS (REST), resource policy, usage plans + API keys.
- **Amazon EMR** — security configurations (KMS for at-rest, Kerberos for in-cluster auth, LDAP for user creds), EMRFS consistent-view deprecated, S3 gateway endpoint, IAM roles for EMR + EC2 + service.
- **AWS IoT Core** — X.509 cert + AWS IoT Device Defender Audit (Device Defender Detect DEPRECATED is closed to new customers since 31 Aug 2026; AWS names no replacement service), IoT policy with `iot:ClientId` condition. Device identity via Just-in-Time Registration or AWS Private CA.

9 · Data Protection

Amazon S3 Protection Patterns

- **Block Public Access** at account + bucket level (default on new buckets). Check with IAM Access Analyzer.
- **Encryption** — SSE-S3 (AES-256), SSE-KMS (CMK, auditable via CloudTrail), SSE-C (customer-provided key), DSSE-KMS (dual-layer, high-compliance). **Bucket Keys** reduce KMS API costs.
- **Bucket policies + ACLs** — prefer bucket policies; ACLs disabled by default (Object Ownership = BucketOwnerEnforced).
- **Object Lock** — WORM; Governance (bypass with perm) or Compliance (truly immutable even for root).
- **Access Points** — per-workload endpoints with own policy + optional VPC-only. Multi-Region Access Points route to closest Region.
- **Presigned URLs** — delegate download/upload with short TTL; inherit caller's IAM.
- **Replication** — SRR/CRR with RTC (15-min SLA); replicate to Log Archive account in different Region for ransomware-resilient logs.
- **Macie** scans for PII; event-driven remediation on findings.

Database & Analytics Protection

- **RDS / Aurora** — at-rest encryption with KMS, in-transit via TLS (`rds.force_ssl` param), IAM database authentication or AWS Secrets Manager rotation, Database Activity Streams for Aurora/RDS to Kinesis.
- **DynamoDB** — at-rest encryption (AWS-owned / AWS-managed / customer-managed KMS), VPC endpoints, fine-grained access with `dynamodb:LeadingKeys`.
- **Amazon OpenSearch** — at-rest + node-to-node + in-transit encryption, fine-grained access (native user, IAM, SAML), VPC-only, audit logs.
- **Athena** — workgroups enforce encryption + CMK; result bucket + query log encryption.
- **SageMaker AI / Bedrock / Amazon Q** — customer data not used for training; data remains in your account; Bedrock Guardrails for PII redaction + denied topics.

Storage Services

- **Amazon EFS** — at-rest KMS; in-transit TLS via mount helper or stunnel; POSIX perms + EFS Access Points + IAM; Lifecycle policies tier to IA/Archive.
- **Amazon FSx for Lustre** — at-rest encryption (SSE-KMS), in-transit encryption within VPC, POSIX via Lustre ACLs, S3 data repository with IAM-gated sync.
- **AWS Backup** — AES-256 at rest with KMS; vaults with access policies + vault lock (WORM); org-wide backup plans via delegated admin.
- **AWS DataSync** — TLS 1.2 in transit; integrates with PrivateLink for fully private transfers. Task reports with data integrity checks.

10 · AWS Security & Compliance Services Matrix

Service	Use
AWS Artifact	Download compliance attestations (SOC, ISO, PCI, HIPAA, FedRAMP) and sign AWS agreements (BAA, DPA).
AWS Audit Manager CLOSED · ON GUIDE	Automated evidence collection mapped to frameworks (PCI, SOC 2, HIPAA, NIST, GDPR, CIS). Closed to new customers since 30 Apr 2026 → Config conformance packs (none for SOC 2, ISO 27001 or GDPR).
AWS Service Catalog	Curated approved stacks (CFN products) for self-service; Launch Constraints + TagOptions enforce guardrails.
AWS CloudFormation	IaC baseline for all security controls; Hooks pre-validate; Guard/cfn-nag as policy-as-code.
AWS Systems Manager	Patch Manager + State Manager for OS hygiene; Session Manager (no SSH); Fleet Manager; Change Calendar; OpsCenter; Parameter Store SecureString. (Change Manager and Incident Manager are closed to new customers.)

11 · Policy Patterns You Must Recognise

S3 bucket deny non-TLS

- Bucket policy Deny when `aws:SecureTransport = false`.

Enforce CMK encryption on new S3 objects

- Bucket policy `Deny s3:PutObject` unless `s3:x-amz-server-side-encryption = aws:kms` AND `s3:x-amz-server-side-encryption-aws-kms-key-id` = your CMK ARN.

Restrict principal by org

- Resource policy condition `aws:PrincipalOrgID = o-xxxx`. Prevents external accounts even if policy accidentally grants `Principal: *`.

Restrict API to specific VPC endpoint

- Resource (or SCP / RCP) condition `aws:SourceVpce = vpce-xxxx`. Service must support it (S3, SQS, SNS, Secrets Manager, KMS).

MFA-required action

- Condition `aws:MultiFactorAuthPresent = true` or `aws:MultiFactorAuthAge < 3600`.

Confused deputy prevention

- In cross-account role trust policy, require `sts:ExternalId` the third party provides and `aws:SourceAccount` / `aws:SourceArn` to match.

Force CloudTrail log integrity

- Enable log-file validation; trail writes SHA-256 digest files + signs with AWS-owned key. `aws cloudtrail validate-logs` detects tampering.

Deny disabling security services

- SCP denies `guardduty:DeleteDetector`, `config:DeleteConfigurationRecorder`, `cloudtrail:StopLogging`, `cloudtrail:DeleteTrail`, `securityhub:DisableSecurityHub`. Critical in every production OU.

12 · Scenario → Answer Patterns

Scenario	Answer
Centralised, tamper-proof logs across Org	Org trail → S3 in Log Archive account with Object Lock Compliance + SSE-KMS + CRR; Security Hub + Config + GuardDuty delegated to Audit account; Security Lake for normalisation.
Remove public S3 object access	Block Public Access at account + bucket; Macie + IAM Access Analyzer for ongoing detection; Config managed rule + SSM Automation for remediation.
Detect anomalous console logins	GuardDuty finding *UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B* + CloudTrail Insights; EventBridge → SSM Automation quarantine.
EC2 compromise: isolate + preserve evidence	Automated Forensics Orchestrator for EC2 or manual: replace SG with quarantine, detach from ASG/TG, snapshot EBS, capture memory via SSM, copy to forensic account.
Enforce encryption with specific CMK on S3 writes	Bucket policy Deny unless `x-amz-server-side-encryption=aws:kms` + `kms-key-id=` that CMK ARN.
Automatic rotation of RDS master creds	Secrets Manager with native rotation Lambda; grant app roles `secretsmanager:GetSecretValue` scoped by ABAC tag.
Share a secret across accounts for a partner	Secrets Manager resource policy granting the partner's IAM role; encrypted with a CMK whose key policy also grants partner.
Prevent deletion of CloudTrail across org	SCP denies `cloudtrail:StopLogging` / `DeleteTrail` / `UpdateTrail`.
Block root user actions in member accounts	SCP with condition `aws:PrincipalType = Root` denying anything except billing.
Prevent data exfiltration to external S3 buckets	Endpoint policy on S3 VPC endpoint limiting buckets; SCP with `aws:ResourceOrgID` restricting S3 targets.
Need to meet PCI DSS — automate evidence	Config Conformance Pack for PCI DSS + Security Hub PCI standard (Audit Manager PCI framework on older answers).
Centrally manage WAF rules across 50 accounts	AWS Firewall Manager policy targeting Org with AWS WAF + Shield Advanced.
Zero-trust internal apps, no VPN	AWS Verified Access with IAM Identity Center / OIDC + device posture (Jamf/CrowdStrike); Verified Permissions for app-level authorisation.
Detect IAM credentials accidentally exposed in a public repo	GuardDuty *UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration*; Inspector Code Security secret scanning (CodeGuru Security on older answers, retired Nov 2025); IAM disable keys + rotate.
Detect ransomware on S3	S3 Versioning + MFA Delete + Object Lock + AWS Backup vault lock; GuardDuty S3 Protection; Macie for anomalous bulk reads.

Scenario	Answer
Private CA hierarchy for mTLS across services	AWS Private CA root + subordinate; issue device / service certs; Enterprise-wide trust store distributed via SSM State Manager.
Prevent IMDSv1 on EC2 fleet	SCP / launch-template enforcement that requires `HttpTokens = required`; Config rule *ec2-imdsv2-check*.
Immutable log chain from on-prem + AWS	Security Lake ingests from AWS + Parquet partner connectors; S3 Object Lock Compliance mode on the lake bucket.
Detect and block DNS tunnelling	Route 53 Resolver DNS Firewall with AWS-managed domain list; Resolver query logs → GuardDuty + CloudWatch.
Require MFA for sensitive admin actions	Identity policy / role trust policy condition `aws:MultiFactorAuthPresent = true`; Session policies for break-glass roles.
Break-glass root access audit	Hardware MFA on root; alarm on root login via CloudWatch metric filter on CloudTrail `userIdentity.type = Root`.
Sensitive keys must never leave HSM boundary	AWS CloudHSM (FIPS 140-2 Level 3); KMS custom key store backed by CloudHSM.

13 · Common Exam Pitfalls

- **SCP does not grant permissions.** Even if an SCP allows everything, identity-based policies still need to grant. SCPs cap, don't grant.
- **Explicit deny always wins** across all policy types. Common trap: an SCP denies but question asks "why can't user do X?" — the SCP is often the answer.
- **Resource policy vs identity policy** — cross-account access needs BOTH: source account's identity policy allows, destination resource policy allows.
- **CMK key policy must grant account root** for IAM policies on that key to have any effect. Missing root grant = locked-out key.
- **S3 Block Public Access overrides everything** — policies, ACLs. Even with a bucket policy granting public, BPA denies.
- **VPC endpoint policies are *not* SG rules** — they're IAM-style; if missing or too restrictive, endpoint blocks legitimate API calls silently.
- **KMS grants vs key policies** — grants are temporary delegation; key policy is primary authorisation. Services often use grants internally.
- **CloudTrail Insights vs GuardDuty** — Insights finds unusual API rate / error-rate patterns (management events volume); GuardDuty is behavioural threat detection.
- **Macie finds PII in S3**; it does not scan databases or logs for sensitive data. For DB, use custom data classification.
- **Inspector replaces Amazon Inspector Classic** — answer "new Inspector" scans continuously, Classic ran on-demand.
- **mTLS** — supported on ALB and API Gateway (REST). Provide trust-store in S3 (Private CA bundle).
- **Org trail** applies to all accounts; member accounts cannot modify it. Preferred pattern for governance.
- **Security Lake vs OpenSearch vs Athena** — Security Lake is the normalised OCSF data lake; Athena queries S3; OpenSearch is a searchable + alerting index. They stack, not compete.

SCS-C03 default answers: "Detect + auto-respond" → GuardDuty + EventBridge + SSM Automation. "Central policy across accounts" → Firewall Manager / Organizations SCPs / Security Hub delegated admin. "Protect keys" → KMS CMK with key policy + grants; CloudHSM if FIPS 140-2 Level 3 required. "Prove compliance" → Config Conformance Packs + Security Hub standards (Audit Manager on older answers; closed to new customers). "Tamper-proof logs" → Org trail + Log Archive account + S3 Object Lock Compliance.

14 · IAM Policy Deep Dive

Evaluation Logic (Memorise)

1. If there's an explicit deny anywhere (SCP, RCP, resource policy, identity policy, perm boundary, session policy, VPC endpoint policy) → **DENY**.
2. SCP + RCP must allow (implicit deny if not).
3. For same-account requests: resource policy OR identity policy allows.
4. For cross-account: both identity (caller side) AND resource policy (target side) must allow.
5. Permission boundary must allow (caps identity).
6. Session policy (if present) must allow.
7. VPC endpoint policy must allow (when request goes through endpoint).

Key Condition Operators

Operator	Use
`StringEquals`, `StringNotEquals`	Exact match (case-sensitive).
`StringLike`, `StringNotLike`	Wildcards `*` / `?`.
`ArnEquals`, `ArnLike`	Match ARNs with wildcards; safer than StringLike for ARNs.
`IpAddress`, `NotIpAddress`	CIDR source IP.
`Bool`	MFA present, Secure Transport.
`DateGreaterThan`, `DateLessThan`	Token age / request window.
`Null`	Key present or not (e.g., `aws:TokenIssueTime = false` = non-STS caller).
`NumericLessThan`	MultiFactorAuthAge < 3600.
IfExists suffix	Evaluate only if key present; useful for optional ABAC tags.
ForAllValues / *ForAnyValue*	Multi-valued condition keys (tags, groups).

Trust Policy Pattern (Cross-Account)

The classic pattern: prevent the "confused deputy" where account A impersonates one of A's customers to B.

- In the trust policy for the role in Account B, include `sts:ExternalId` condition with a secret shared with legitimate caller.
- For AWS services accessing your account (e.g., S3 notifications to SNS in another account), use `aws:SourceAccount` + `aws:SourceArn`.
- Prefer unique role per consumer; limit `Principal` to specific roles/accounts (never `*`).

15 · KMS Key Policy Deep Dive

Anatomy of a Usable Key Policy

- **Enable IAM policies** — required statement granting `kms:*` to account root; without it the key is locked out.
- **Key administrators** — statement limiting admin actions (`kms:Create*`, `kms:Describe*`, `kms:PutKeyPolicy`) to an admin role; no cryptographic use.
- **Key users** — statement granting `kms:Encrypt`, `kms:Decrypt`, `kms:ReEncrypt*`, `kms:GenerateDataKey*`, `kms:DescribeKey`.
- **Service use (via grants)** — `kms:CreateGrant` granted to integrated service principals.

Common Traps

- **Cross-account key use** — key policy grants other account (`Principal: "arn:aws:iam::111:role/app"`) AND identity policy in that account grants `kms:*` on the key ARN.
- **Pipeline artefact encrypted with CMK** — CodePipeline artefact bucket uses CMK; target account role must be in key policy (`Decrypt`, `GenerateDataKey`).
- **S3 + SSE-KMS cross-account** — bucket policy + IAM policy + KMS key policy all must allow.
- **Disabled keys** — cannot decrypt; takes 24 h minimum to delete after scheduling (up to 30 days).
- **Key rotation** — auto-rotation generates new key material; older material retained to decrypt old ciphertext. Manual rotation = new CMK + re-encrypt DEKs.

16 · Logging & Detection Reference Architectures

Org-wide Logging & Forensics

- **Organization CloudTrail** — one trail, created in management, delivers every account's events to the Log Archive S3 bucket. Encrypted with CMK whose policy grants CloudTrail service.
- **S3 Object Lock Compliance** on log bucket; Versioning + MFA Delete on sensitive data buckets.
- **Cross-Region replication** of the log bucket to a second Region + second account for ransomware resilience.
- **CloudTrail Lake event data store** CLOSED · ON GUIDE for SQL-based forensics (up to 10 years); closed to new customers, so a new design queries trail logs in S3 with Athena or uses CloudWatch.
- **AWS Config + Conformance Pack** deployed org-wide; aggregator in Audit account.
- **Security Lake** consuming CloudTrail, VPC Flow, Route 53 Resolver query logs, EKS audit, Security Hub findings; subscribers (Athena / OpenSearch / SIEM) query OCSF Parquet.

Detection Pipeline

- GuardDuty delegated admin in Audit → findings go to Security Hub delegated admin.
- Security Hub aggregates + standards evaluation; findings flow to EventBridge rules.
- Critical findings → SSM Automation quarantine (replace SG, detach from TG, snapshot EBS).
- All findings → Security Lake (via Security Hub → EventBridge → Firehose → S3 OCSF).
- On-call paged via a partner paging tool (Incident Manager is closed to new customers); Slack/Teams via User Notifications + Chatbot.

17 · Specialised Workload Security

AWS Lambda

- Execution role scoped to specific resources; prefer session policies for short-lived access.
- Env vars encrypted at rest with account-level KMS key; use customer-managed key + KMS decrypt permission.
- Signed deployment packages via AWS Signer; code signing config on function enforces.
- Invoke resource policy restricts which principals/services can invoke.
- Inspector continuously scans function code + layers for CVEs.

Amazon EKS

- **IAM + RBAC** — aws-auth ConfigMap maps IAM to K8s users/groups. Prefer Access Entries (newer) with Access Policies.
- **Pod identities** — IRSA or EKS Pod Identity Agent; pods assume role without node creds.
- **Network policies** — VPC CNI + Calico or Cilium; Security Groups for Pods.
- **Control plane audit** → CloudWatch Logs; ingest to Security Lake.
- **Runtime** — GuardDuty EKS Runtime Monitoring (syscall telemetry via eBPF); Inspector scans pod images.

Amazon SageMaker AI & Bedrock & Amazon Q

- **SageMaker** — network isolation mode for training jobs, VPC endpoints, notebook root-access disable, IAM role per execution, encrypted EBS/FSx, customer-managed KMS.
- **Bedrock** — guardrails (content filters, denied topics, PII redaction, prompt-injection checks, grounding); customer data never used for training by default; PrivateLink endpoint for VPC-only access.
- **Amazon Q Developer** END OF SUPPORT · ON GUIDE — IDE plugins and Pro subscriptions reach end of support 30 Apr 2027 (Q in the AWS console continues) and the CLI is now Kiro. Until then, the Pro tier: content not used for service improvement; admin controls; IAM Identity Center authentication; code reviews with SAST + secrets detection.
- **Amazon Q Business** CLOSED · ON GUIDE — on the guide but closed to new customers (→ Amazon Quick). Admin-controlled data sources, ACL-aware answers, IAM Identity Center authentication.
- **Amazon CodeGuru Security** RETIRED — static analysis for IAM, secrets, insecure crypto, log injection. End of support 20 Nov 2025 (still on the guide) → Amazon Inspector Code Security (SAST, secrets, IaC on GitHub / GitLab repos).

AWS IoT Core

- Device identity via X.509 cert (JITP / JITR) or Private CA. IoT policy condition on `iot:ClientId` and topic patterns.
- IoT Device Defender Audit checks the fleet (policy too permissive, shared cert). Device Defender Detect DEPRECATED (anomalies such as auth failures or message spikes) is closed to new customers since 31 Aug 2026; AWS names no replacement service, only a self-managed sample pipeline.

18 · Compliance Frameworks Mapped to AWS

Framework	AWS primary controls
PCI DSS v4	AWS PCI DSS Level 1. Security Hub PCI standard; Config conformance pack for PCI DSS; KMS + CloudHSM for key lifecycle; WAF for L7; VPC segmentation.
HIPAA	BAA via AWS Artifact; use HIPAA-eligible services only; encrypt at rest + in transit; CloudTrail Management + Data events; Macie for PHI in S3.
SOC 2	CloudTrail + Config + Security Hub FSBP; Change Calendar + approvals in Automation. No Config conformance pack for SOC 2 (Audit Manager and Change Manager are closed to new customers).
FedRAMP (Moderate / High)	AWS GovCloud (High) or standard commercial (Moderate); limit services to those authorised at your impact level.
ISO 27001	Continuous config evaluation with Config rules + Security Hub. No Config conformance pack for ISO 27001 (Audit Manager is closed to new customers).
NIST 800-53 Rev 5	Security Hub NIST 800-53 standard; Conformance Pack.
GDPR	Data residency via Region selection; encryption; DPA via Artifact; data-subject request automation with Macie + Lake Formation + S3 Inventory.

19 · Step-by-Step Runbooks

Compromised IAM Access Key

1. Mark the key inactive in IAM (`aws iam update-access-key --status Inactive`).
2. Rotate: create new key, update apps, delete old one.
3. Check CloudTrail for actions performed under the key; GuardDuty finding type *InstanceCredentialExfiltration* suggests automation.
4. If key was for a service account, migrate to role-based access (IRSA / instance profile / IAM role).
5. Scan code repos with Inspector Code Security / git-secrets.

Public S3 Bucket with Sensitive Data

1. Enable Block Public Access at account + bucket immediately.
2. Revoke grants via S3 Object Ownership = BucketOwnerEnforced (disables ACLs).
3. Run Macie scan on the bucket for sensitive-data discovery.
4. Notify legal / privacy + log customer incidents.
5. Config rule *s3-bucket-public-read-prohibited* + SSM Automation auto-remediation to prevent regression.

Root Account Misuse

1. CloudWatch metric filter on CloudTrail `$.userIdentity.type = "Root"` → alarm → SNS.
2. On alarm: notify CISO + security on-call; freeze billing changes; rotate root password + hardware MFA.
3. Audit sequence of actions in CloudTrail.
4. Enforce SCP: deny all but billing-read for root; Control Tower guardrail.

Suspicious Cross-Account STS Assumptions

1. Check IAM Access Analyzer external findings — any roles trusting unexpected accounts?
2. Review CloudTrail for `sts:AssumeRole` events, source IP, ExternalId match.
3. If malicious: revoke all active sessions via IAM role policy "revoke active sessions" action; rotate role trust policy.
4. Add `aws:SourceAccount` + `ExternalId` conditions to prevent recurrence.

20 · Retired, Closed or End of Support

Older questions and study material still name these. Know what they did; for a new design, pick the replacement.

Service	Status → What to use instead
Amazon CodeGuru Security RETIRED	End of support 20 Nov 2025 (still on the guide) → Amazon Inspector Code Security.
Amazon Q Business CLOSED · ON GUIDE	No longer open to new customers → Amazon Quick.
Amazon Q Developer END OF SUPPORT · ON GUIDE	IDE plugins + Pro end of support 30 Apr 2027 (console unaffected); the CLI is now Kiro → Kiro.
AWS Audit Manager CLOSED · ON GUIDE	Closed to new customers since 30 Apr 2026 → Config conformance packs (none for SOC 2, ISO 27001 or GDPR).
CloudTrail Lake CLOSED · ON GUIDE	Closed to new customers since 31 May 2026 → CloudWatch, or trail logs in S3 queried with Athena.
AWS IoT Device Defender Detect DEPRECATED	Closed to new customers since 31 Aug 2026. AWS names no replacement service (only a self-managed sample pipeline). Device Defender Audit stays available.
Systems Manager Incident Manager DEPRECATED	Closed to new customers since 7 Nov 2025 → Systems Manager OpsCenter, or partner paging (PagerDuty, Jira Service Management, ServiceNow).
Systems Manager Change Manager DEPRECATED	Closed to new customers since 7 Nov 2025 → partner ITSM tool (AWS names no AWS successor).
Simple AD DEPRECATED	Closed to new customers → AWS Managed Microsoft AD, or AD Connector.
AWS App Runner DEPRECATED	Closed to new customers → Amazon ECS Express Mode.
Amazon Inspector Classic RETIRED	Shut down 20 May 2026 → Amazon Inspector.

Built by **CloudNinja** · **cloudninja.pro** · Free AWS practice exams & cheat sheets. No signup, no paywall.