

AWS Security Services - Keyword Cheat Sheet

Service / Topic	Exam Keywords	Main Uses
Amazon KMS	Managed encryption, CMKs, envelope encryption, FIPS 140-2, integrated services	Create/manage encryption keys, encrypt data (S3, EBS, RDS), envelope encryption, auditing via CloudTrail
AWS CloudHSM	Dedicated HSM, single-tenant, compliance, FIPS 140-2 Level 3	Hardware-based key storage, customer-exclusive control, compliance (PCI DSS, HIPAA), integrates with KMS
AWS Abuse	Abuse report, phishing, DDoS, compromised resources, spam	Report malicious/abusive activity, compromised instances, phishing, malware (via abuse@amazonaws.com)
Amazon Cognito	Authentication, authorization, identity federation, SAML, OIDC, MFA	User auth for apps, supports sign-up/sign-in, MFA, integrates with social & enterprise IdPs, temporary AWS creds
Amazon Macie	Data discovery, PII, sensitive data, ML-driven, S3	Discover/classify sensitive data, automate compliance checks, alerts on unencrypted/public data
AWS Security Hub	Centralized security, compliance standards, CIS, PCI DSS, integrations	Aggregates findings (GuardDuty, Macie, Inspector), compliance dashboards, continuous monitoring
AWS Certificate Manager (ACM)	SSL/TLS, managed certificates, free, automatic renewal	Provision/manage SSL/TLS certs, automatic renewal, used with CloudFront, ALB, API Gateway
AWS Systems Manager (SSM)	OpsCenter, Parameter Store, Patch Manager, Run Command, Session Manager	Manage EC2/hybrid environments, patching, remote commands, config/secret mgmt, secure shell access
AWS Audit Manager	Continuous audit, evidence collection, compliance frameworks	Automates audit evidence collection, generates reports, maps controls to compliance standards

Service / Topic	Exam Keywords	Main Uses
AWS Identity & Access Management (IAM)	Identities, users, groups, roles, least privilege, root account, temporary creds	Manage AWS users & permissions, assign least privilege, enable secure access with roles and policies
IAM Infrastructure	Global service, root user, users, groups, roles, policies	Defines AWS identity system, roles for services/applications, global (not region-specific)
Multi-Factor Authentication (MFA)	Extra layer of security, virtual/hardware tokens, root account protection	Secure root & IAM users, enforce MFA for login and API calls, protects against credential theft
IAM Policy	JSON policy, effect, action, resource, condition, inline vs managed policies	Define permissions for users, groups, and roles; allow/deny access to AWS resources
IAM Best Practices	Least privilege, MFA, no root user for daily ops, rotate keys, CloudTrail logging	Secure IAM usage, enforce strong security posture, use roles instead of static keys
Shared Responsibility Model	AWS secures cloud of (infra, hardware, global network), customer secures cloud in (data, apps, config)	Defines division of security duties: AWS manages physical infra, customer manages data, IAM, encryption, patches
AWS CloudTrail	API activity logging, governance, auditing, compliance	Logs all API calls/events in AWS, detects changes, integrates with CloudWatch for alerts
Amazon CloudWatch	Monitoring, metrics, alarms, logs, dashboards	Collects metrics/logs, monitors applications/resources, sets alarms, automates responses
AWS Shield	DDoS protection, Standard (free), Advanced (paid)	Protects apps from DDoS attacks, integrates with CloudFront/Route53, Advanced includes 24/7 support

Service / Topic	Exam Keywords	Main Uses
Amazon GuardDuty	Threat detection, ML/anomaly detection, malicious activity	Monitors AWS accounts/logs for suspicious behavior, integrates with Security Hub, sends actionable alerts
Amazon Inspector	Vulnerability management, EC2/ECR scanning, CVE detection	Scans workloads for vulnerabilities, checks against best practices, integrates with Security Hub
Amazon Trusted Advisor	Best practice checks, cost optimization, security gaps, service limits	Provides recommendations for security, cost, performance, service quotas
AWS Network Firewall	Managed network firewall, VPC-level, stateful/stateless rules	Protects VPC traffic with advanced network filtering, intrusion detection/prevention
AWS Firewall Manager	Centralized firewall policy management, multi-account, org-wide	Manage WAF, Shield Advanced, and Network Firewall policies across multiple AWS accounts
Amazon WAF	Web Application Firewall, layer 7 protection, OWASP Top 10	Protects web apps from SQL injection, XSS, bots; integrates with CloudFront, ALB, API Gateway