AWS Cloud Security

SHARED RESPONSIBILITY · IAM · ACCOUNT HARDENING · ACCOUNT SERVICES · DATA PROTECTION · COMPLIANCE STUDY & REVIEW

01 MUST KNOW

if you remember five things, remember these

01 **Shared responsibility:** AWS secures the cloud itself — security **OF** the cloud (facilities, hardware, network, virtualization). You secure everything you put in it — security **IN** the cloud (OS, apps, data, IAM, firewall rules).

02 **IAM** = **users** (long-term identity), **groups** (policy attached to many users), **roles** (temporary credentials), **policies** (JSON allow/deny). IAM is a **global** service — never tied to a Region.

03 **Policy evaluation:** everything starts **implicitly denied** → an allow grants access → an **explicit deny always wins**, no matter what else allows.

04 **New-account hardening:** root gets MFA → root access keys deleted → individual IAM users created → CloudTrail on → billing reports on → password policy set. Root retires from daily work.

05 **Roles over keys:** apps on EC2 should get permissions by **assuming a role** (temporary credentials), never from access keys stored on the instance.

02 KEY TERMS

TERM	DEFINITION
Shared responsibility	AWS: security of the cloud · customer: security in the cloud
IAM user	Long-term identity for one person or application
IAM group	Collection of users; attach one policy to many (groups can't nest)
IAM role	Assumable identity that issues temporary security credentials
Identity-based policy	JSON permissions doc attached to a user, group, or role
Resource-based policy	Policy attached to a resource, e.g. an S3 bucket policy
Principle of least privilege	Grant only the permissions required to do the task
MFA	Second sign-in factor; non-negotiable for the root user
Root user	Account owner identity with unrestricted access — protect and shelve it
SCP (service control policy)	Org-level cap on member-account permissions; never grants
AWS KMS	Creates/manages encryption keys on FIPS 140-2 validated HSMs
AWS CloudTrail	Records API calls made in the account (who did what, when)

03 WHO SECURES WHAT

AWS — OF THE CLOUD

the infrastructure that runs everything

- Physical data centers, hardware, facilities
- Hypervisor / virtualization layer
- Global network infrastructure
- Software underlying managed services (RDS, Lambda, DynamoDB)

CUSTOMER — IN THE CLOUD

everything you configure and upload

- Guest OS on EC2: updates & security patches
- Security groups / firewall configuration
- IAM users, credentials, permissions
- Application code, customer data, encryption choices

04 RESPONSIBILITY BY SERVICE MODEL

the more managed the service, the more AWS carries

MODEL	WHO DOES WHAT	EXAMPLES
IaaS	Customer has most flexibility and most security duties: OS patching, security groups, access control	Amazon EC2
PaaS	AWS runs OS, patching, firewall, disaster recovery; customer manages data, asset classification, permissions	AWS Lambda, Amazon RDS
SaaS	Centrally hosted software, subscription or pay-as-you-go; customer manages only data + access	Trusted Advisor, AWS Shield, Amazon Chime

05 SECURITY SERVICES AT A GLANCE

know each one's one-line job

SERVICE	WHAT IT DOES	REMEMBER
IAM	Users, groups, roles, policies for authN + authZ	Global · free
Organizations	Consolidate + centrally manage multiple accounts, group into OUs	Permissions = SCP ∩ IAM
SCPs	JSON caps on maximum permissions of member accounts	Never grant — only limit
KMS	Create/manage/rotate encryption keys; integrates with CloudTrail	FIPS 140-2 HSMs
Cognito	Sign-up / sign-in / access control for web & mobile apps	Social + SAML federation
Shield	Managed DDoS protection	Standard: free, always on
CloudTrail	Logs every API call (who, what, when)	Enable in all Regions
Config	Records + evaluates resource configurations vs. rules	It's a **Regional** service
Artifact	On-demand security & compliance reports and agreements	ISO, PCI, SOC, BAA
Service Catalog	Catalogs of org-approved IT products with constraints	Governance tool
Macie	ML discovery + protection of PII in S3	Data classification
Inspector	Automated security assessments of deployed apps	Findings by severity
GuardDuty	Intelligent threat detection over CloudTrail / VPC Flow / DNS logs	Continuous monitoring

06 SECURING A NEW ACCOUNT, IN ORDER

01 **Root MFA** on → 02 **Delete** root access keys → 03 Create **IAM users** (+ groups) → 04 **CloudTrail** on in all Regions → 05 **Billing reports** on → 06 **Password policy** set → 07 Root **retired** from daily use

07 PROTECTING DATA

encryption is always the customer's call to enable

DATA STATE	HOW IT'S PROTECTED
At rest	AES-256 via AWS KMS — supported by S3, EBS, EFS, RDS; transparent once enabled
In transit	TLS (formerly SSL); AWS Certificate Manager issues + renews certificates; HTTPS = encrypted tunnel
In S3	Buckets & objects **private by default** · Block Public Access · bucket policies · least-privilege + encryption when sharing

08 EXAM TRAPS

where the knowledge check gets you

- × “IAM is a regional service.” — **False.** IAM is global; users, groups, and policies apply account-wide.
- × “An allow anywhere grants access.” — Only when **no explicit deny** exists anywhere. Deny is final.
- × “SCPs grant permissions to member accounts.” — SCPs **never grant**; they cap. Effective permissions = what SCP allows ∩ what IAM grants.
- × “AWS encrypts my data for me.” — *Enabling* encryption of your data is **your** responsibility, even on managed services.
- × “AWS patches my EC2 instances.” — You patch the **guest OS** on EC2. AWS patches the OS/database under managed services like RDS.
- × “New S3 buckets are public.” — New buckets and objects are **private and protected by default**.
- × “Shield costs extra.” — Shield **Standard** is automatic and free for all customers; only Shield **Advanced** is a paid option.
- × “AWS Config is global like IAM.” — Config is **Regional**; enable it per Region (an aggregator can combine views).

09 SELF-QUIZ

answers are upside-down below

Q1 Under the shared responsibility model, who patches the guest OS on an EC2 instance?

Q2 Name the four core IAM components.

Q3 A user's policies contain an allow and an explicit deny for the same action. Net result?

Q4 Which policy type sets a maximum on what member accounts can do but never grants anything?

Q5 Which service records every API call made in your account?

Q6 Which DDoS protection tier is automatically enabled, at no cost, for every AWS customer?

Q7 Which encryption algorithm does AWS use for data at rest, and which service manages the keys?

Q8 Where do you download AWS ISO / PCI / SOC compliance reports on demand?

Q9 Which service adds sign-up, sign-in, and access control to your web and mobile apps?

Q10 Sample CCP exam: which of these is AWS's responsibility — configuring third-party apps, maintaining physical hardware, securing application access and data, or managing custom AMIs?

ANSWER KEY (rotate the page)

Q1 the customer **Q2** users, groups, roles, policies **Q3** denied — explicit deny always wins **Q4** service control policy (SCP) **Q5** AWS CloudTrail **Q6** AWS Shield Standard **Q7** AES-256, keys in AWS KMS **Q8** AWS Artifact **Q9** Amazon Cognito **Q10** maintaining physical hardware