Introduction to Security on AWS

CLOUD SECURITY BENEFITS · CIA TRIAD · SECURITY OBJECTIVES & SERVICES · SEVEN DESIGN PRINCIPLES · SHARED RESPONSIBILITY · MSO

STUDY & REVIEW

01 MUST KNOW

if you remember five things, remember these

01 **Security is familiar:** cloud security protects the same **confidentiality, integrity, and availability (CIA)** you protect on premises — only with **software-based tools** instead of guarding physical facilities and hardware. AWS lets you bring your existing security models (visibility, auditability, controllability) to the cloud and adds agility and automation on top.

02 **Five objectives → services: controllability** → IAM, STS, CloudHSM · **auditability** → CloudTrail · **visibility** → Config · **agility and automation** → CloudFormation. Each objective answers a specific security question about who, what, when, and where regarding your AWS resources.

03 **Seven design principles:** from the **security pillar of the AWS Well-Architected Framework** — apply least privilege, enable traceability, secure all layers (defense in depth), automate security, protect data in transit and at rest, prepare for security events, and minimize the attack surface.

04 **Security OF vs IN the cloud: AWS secures the cloud** — the hardware, software, networking, and facilities of the Global Infrastructure, plus the host OS and virtualization (hypervisor) layer. **You secure what you put in the cloud** — guest OS, applications, IAM, security groups, data, and encryption.

05 **The split moves with your services:** the more managed the service, the more AWS handles. AWS patches an Oracle database on **Amazon RDS**; *you* patch the same Oracle if it runs on an **EC2 instance**. Configuring security groups, VPCs, SSH keys, and MFA is always the **customer's** job.

02 KEY TERMS

TERM	DEFINITION
Confidentiality	Limiting information access and disclosure to authorized users and preventing access by unauthorized people
Integrity	Maintaining the consistency, accuracy, and trustworthiness of data over its entire lifecycle, at rest and in transit
Availability	The readiness of information resources — having access to information when it is needed
AWS IAM	Identity and Access Management: controls who can use AWS resources (authentication) and what they can do and how (authorization) via granular permissions for users, groups, and roles
AWS STS	Security Token Service: creates and provides trusted users with temporary security credentials for controlled access to AWS resources
AWS CloudHSM	Protects your encryption keys inside hardware security modules validated to government standards, so only you can access the keys
AWS CloudTrail	Records API calls and account activity to answer who took what action, when, and from what source IP — the basis for auditing
AWS Config	Discovers resources, exports a full inventory with configuration details, and shows how a resource was configured at any point in time
AWS CloudFormation	Deploys environments as code (infrastructure as code) in a secure, reproducible manner; used to pre-provision forensic clean rooms
Shared responsibility model	Division of security duties: AWS is responsible for security OF the cloud; the customer is responsible for security IN the cloud
Defense in depth	Applying security controls at every layer (network, application, data store) rather than only the outer perimeter

TERM	DEFINITION
Security group	A customer-configured virtual firewall that filters instance traffic by protocol and port number, controlling network access to EC2 and RDS

03 AWS CLOUD SECURITY OBJECTIVES → SERVICES

each objective answers a question, and AWS provides a service for it

OBJECTIVE	THE QUESTION IT ANSWERS	AWS SERVICE
Controllability	Can I manage users? Provide temporary credentials? Use my own keys?	IAM · STS · CloudHSM
Auditability	Who has access? Who performed what action, when, and from where?	CloudTrail
Visibility	What is in my environment? What changed, and what impact did it have?	Config
Agility & automation	How do I ensure high availability and apply security checks reproducibly?	CloudFormation

04 SHARED RESPONSIBILITY MODEL

security and compliance are shared

AWS — SECURITY OF THE CLOUD

AWS operates, manages, and controls

- Physical security of facilities and data centers
- Hardware and the AWS Global Infrastructure — Regions, Availability Zones, edge locations
- Host operating system and virtualization (hypervisor) layer
- Networking infrastructure and isolation between customers
- Foundation services: compute, storage, databases, networking

CUSTOMER — SECURITY IN THE CLOUD

you secure what you put in the cloud

- Customer data, encryption options, and data integrity
- Platform, applications, and IAM
- Guest OS configuration, updates, and security patches
- Network and firewall config — security groups, VPC, subnets
- Client-side and server-side encryption; traffic protection

05 THE SEVEN SECURITY DESIGN PRINCIPLES

from the AWS Well-Architected security pillar

PRINCIPLE	WHAT IT MEANS
1. Apply least privilege	Deny by default; grant access only as needed by job role; separation of duties; avoid long-term credentials (use roles, SSO/federation, MFA)
2. Enable traceability	Monitor, alert, and audit actions and changes in near-real time with logs and metrics — CloudTrail, CloudWatch, Config, GuardDuty
3. Secure all layers	Defense in depth — controls on the network, application, and data-store layers, not just the perimeter; persist hardened config to immutable AMIs
4. Automate security	Automate routine security tasks with APIs; turn infrastructure into code (CloudFormation) for reproducible, trusted environments
5. Protect data in transit and at rest	Encryption and fine-grained access controls; classify data with tags; use VPN and TLS; SSE for S3, ELB SSL termination
6. Prepare for security events	Put response tools and access in place ahead of time; practice with game days; pre-provision a clean room with CloudFormation
7. Minimize the attack surface	Harden the OS and reduce components; configure security groups and network ACLs in the VPC; scale to absorb attacks (Auto Scaling, CloudFront)

06 WHO IS RESPONSIBLE? (ACTIVITY)

answers to the shared-responsibility scenarios

AWS IS RESPONSIBLE FOR	CUSTOMER IS RESPONSIBLE FOR
the infrastructure and its isolation	*everything they configure and connect*
— Physical security of the data center	— Guest OS upgrades and patches on EC2
— Virtualization infrastructure	— EC2 security group settings; the VPC and subnet
— Oracle patches when Oracle runs on Amazon RDS	— Applications running on the EC2 instance
— Protecting against network outages in AWS Regions	— Oracle patches when Oracle runs on an EC2 instance
— Network isolation between customers; low-latency links	— S3 bucket access configuration; securing SSH keys
— Ensuring the AWS Management Console is not hacked	— Enforcing MFA for all user logins

07 EXAM TRAPS

where the knowledge check gets you

- × "AWS secures everything in the cloud, so I don't have to." — AWS secures the cloud (infrastructure); *you* secure everything you put **in** it — guest OS, applications, data, IAM, and security groups.
- × "The shared responsibility split is fixed." — It **changes with the services you use**. Managed services (Amazon RDS) shift patching to AWS; self-managed workloads (Oracle on EC2) keep OS and database patching with the customer.
- × "AWS patches the guest OS on my EC2 instances." — No — the customer patches the guest OS and applications. AWS patches the **hypervisor and below**.
- × "Configuring security group rules is AWS's responsibility." — Security groups control network access to your instances; **configuring them is a customer responsibility** (this is the module's sample-exam answer).
- × "Cloud security means I still have to protect physical hardware." — In the cloud you use **software-based tools**; AWS owns the physical facilities, hardware, and networking.
- × "Least privilege means giving trusted staff broad access." — Start by **denying access to everything** and grant only as needed by job role; enforce separation of duties and avoid long-term credentials.
- × "Enforcing MFA for user logins is up to AWS." — Enforcing MFA for all user logins is a **customer** responsibility, just like securing SSH keys and configuring the VPC.
- × "Keeping the AWS Management Console from being hacked is my job." — Protecting the global infrastructure and its services — the console, Region availability, and isolation between customers — is **AWS's** responsibility.

08 SELF-QUIZ

answers are upside-down below

Q1 Name the three components of the triad that underlies information security.

Q2 Which AWS service is the primary tool for controlling who can access AWS resources and what they can do?

Q3 Which AWS service provides trusted users with temporary security credentials?

Q4 Which service lets you protect and manage encryption keys inside hardware modules validated to government standards?

Q5 Which AWS service answers who performed what action, when, and from where — supporting auditability?

Q6 Which service gives you a complete inventory and configuration history of your resources for visibility?

Q7 Which service lets you deploy environments as code in a secure, reproducible manner?

Q8 Which design principle says to grant access only as needed, enforce separation of duties, and avoid long-term credentials?

Q9 If an Oracle database runs on an EC2 instance, who is responsible for its upgrades and patches?

Q10 Sample exam: under the shared responsibility model, who configures security group rules that determine which ports are open to an EC2 Linux instance?

ANSWER KEY (rotate the page)

Q1 confidentiality, integrity, availability (CIA) **Q2** AWS IAM (Identity and Access Management) **Q3** AWS STS (Security Token Service) **Q4** AWS CloudHSM **Q5** AWS CloudTrail **Q6** AWS Config **Q7** AWS CloudFormation **Q8** apply the principle of least privilege **Q9** the customer (AWS patches Oracle only when it runs as an Amazon RDS instance) **Q10** the customer (choice B)