CERTIFICATION EXAM PREP · CLF-C02

AWS Certified Cloud Practitioner

Complete Study Guide · All 4 exam domains

Renata R Silva (Maki) @renatarsilvax is a software engineer, tech content creator and 2x AWS certified (Cloud Practitioner and AI Practitioner). Passionate about communities, she actively shares her software engineering and cloud computing study routine on social media.

Introduction

This guide follows the **official AWS Certified Cloud Practitioner (CLF-C02) exam guide**, domain by domain, with contrast tables, trigger words, common traps and a quick summary at the end of each domain. The content was built from official AWS pages (full list in the **Sources** section at the end).

Exam domains

Domain	Weight
1. Cloud Concepts	24%
2. Security and Compliance	30%
3. Cloud Technology and Services	34%
4. Billing, Pricing, and Support	12%

About the exam (official guide)

- 65 questions: **50 scored** and 15 unscored (not identified), in 90 minutes.
- Question types: multiple choice (1 correct, 3 incorrect) and multiple response (2 or more correct out of 5 or more options).
- Unanswered questions are scored as incorrect; **there is no penalty for guessing**.
- Result: scaled score from 100 to 1,000; **minimum passing score is 700**. Compensatory scoring: you do not need to pass each section, only the exam as a whole.
- Target candidate: up to 6 months of AWS Cloud exposure. Out of scope: coding, designing cloud architecture, troubleshooting, implementation and load testing.

Domain 1: Cloud Concepts (24%)

Official task statements: 1.1 benefits of the AWS Cloud · 1.2 design principles · 1.3 migration · 1.4 cloud economics.

1.1 Benefits of the AWS Cloud

Cloud computing is on-demand access to IT resources over the internet, paying only for what you use. AWS summarizes the value proposition in **six advantages**:

#	Advantage	Official description (summarized)
1	**Trade fixed expense for variable expense**	Instead of investing heavily in data centers and servers before you know how you will use them, you pay only when you consume and only for how much you consume.
2	**Benefit from massive economies of scale**	The usage of hundreds of thousands of customers is aggregated, which leads to lower pay-as-you-go prices than you could achieve on your own.
3	**Stop guessing capacity**	Avoids expensive idle resources or limited capacity; scale up and down with just a few minutes of notice.
4	**Increase speed and agility**	New resources are a click away, reducing the time to make them available from weeks to minutes; experimenting costs less.
5	**Stop spending money running and maintaining data centers**	Focus on customers and on what differentiates the business, not on racking, stacking, and powering servers.
6	**Go global in minutes**	Deploy in multiple Regions with a few clicks, with lower latency and a better experience for customers.

Global infrastructure, high availability, elasticity, and agility

Concept	What it means
Global infrastructure	Speed of deployment and global reach (Regions, Availability Zones, edge locations). Details in Domain 3.
High availability	The application keeps operating even with failures, by distributing resources across **multiple Availability Zones**.
Elasticity	Ability to increase and decrease resources according to demand (e.g., Amazon EC2 Auto Scaling).
Agility	Provision and experiment quickly, with a low cost of trial and error.

> **Service and deployment models (foundational concepts).** IaaS: you manage the OS, application, and data (e.g., Amazon EC2). PaaS: the platform is managed, you take care of the application and data (e.g., AWS Elastic Beanstalk). SaaS: ready-made application. Deployment: **cloud**, **hybrid** (cloud + on-premises, e.g., AWS Outposts, Direct Connect, VPN), and **on-premises**.

1.2 Design principles: AWS Well-Architected Framework

The Framework helps you understand the pros and cons of decisions when building systems in the cloud, across **six pillars**. The **AWS Well-Architected Tool** is available at **no cost** in the AWS Management Console and is used to review workloads regularly, identify high risks, and record improvements.

Pillar	Focus (official description)	Trigger words
Operational Excellence	Run and monitor systems and continually improve processes and procedures.	operate, monitor, improve processes
Security	Protect information and systems: data confidentiality, user permissions, threat detection.	protect, permissions
Reliability	Workloads that perform their intended function and recover quickly from failures.	recover from failures
Performance Efficiency	Structured and streamlined allocation of IT and computing resources.	use the right resource
Cost Optimization	Avoid unnecessary costs: spend awareness and correct sizing (rightsizing).	reduce spending
Sustainability	Minimize the environmental impacts of running cloud workloads.	environmental impact

> **Trap:** questions ask you to *tell the pillars apart*. Identify the trigger word in the scenario (recovery, cost, environmental impact, permissions) before looking at the answer choices.

1.3 Migration to the AWS Cloud

AWS Cloud Adoption Framework (AWS CAF)

The CAF uses AWS experience and best practices to help with digital transformation. It is used to identify and prioritize opportunities, assess and improve cloud readiness, and iteratively evolve the roadmap. Business outcomes cited in the exam guide: **reduce business risk, improve ESG performance, grow revenue, and increase operational efficiency**.

Perspective	Focus (official description)	Common stakeholders
Business	Ensure that cloud investments accelerate digital transformation ambitions and business outcomes.	CEO, CFO, COO, CIO, CTO
People	Bridge between technology and business: culture, organizational structure, leadership, and workforce.	CIO, COO, CTO, cloud director
Governance	Orchestrate cloud initiatives while maximizing benefits and minimizing transformation risks.	Chief transformation officer, CIO, CTO, CFO, CDO, CRO
Platform	Build a scalable hybrid cloud platform, modernize workloads, and implement cloud-native solutions.	CTO, technology leaders, architects, engineers
Security	Confidentiality, integrity, and availability of data and workloads in the cloud.	CISO, CCO, internal audit, security architects
Operations	Ensure that cloud services are delivered at the level the business needs.	Infrastructure and operations leaders, SREs, IT service managers

> **Four iterative phases of the journey: Envision** (show how the cloud accelerates business outcomes) → **Align** (identify capability gaps across the six perspectives and align stakeholders) → **Launch** (deliver pilots in production) → **Scale** (expand pilots and ensure sustained benefits).

The 7 migration strategies (7 Rs)

Strategy	Definition (AWS Prescriptive Guidance)	Example
Retire	Decommission or archive applications; lets you turn off the servers in the stack.	"Zombie" applications (average CPU and memory below 5%) or with no inbound connection in 90 days
Retain	Keep in the source environment or do not migrate yet.	Data residency requirement; specialized hardware; recently upgraded
Rehost (lift and shift)	Move to AWS without changing the application.	On-premises application stack to the cloud, with no changes
Relocate	Transfer many servers at once from an on-premises platform to the cloud version of the same platform, or move instances/objects to another VPC, Region, or account. Requires no new hardware or rewrite.	On-premises VMware to VMware Cloud on AWS; RDS instance to another VPC or account
Repurchase (drop and shop)	Replace with a different version or product.	Traditional license to SaaS
Replatform (lift, tinker and shift)	Migrate with some optimization to operate efficiently or reduce cost.	Microsoft SQL Server to Amazon RDS for SQL Server
Refactor / Re-architect	Change the architecture to take advantage of cloud-native features. This is the most complex and costly strategy.	Legacy monolith redesigned for the cloud

> In large migrations, AWS recommends rehost, relocate, replatform, and retire, and modernizing (refactor) **after** the migration.

Migration support resources

Service	What it is for
AWS Migration Hub	Track migration progress in one place.
AWS Application Discovery Service	Discover on-premises servers and applications and their dependencies.
AWS Application Migration Service	Automated rehost of servers to AWS.
AWS Database Migration Service (AWS DMS)	Migrate and replicate databases (includes **database replication**, cited in the exam guide).
AWS Schema Conversion Tool (AWS SCT)	Convert the schema in migrations between different engines.
Migration Evaluator	Support the business case and migration estimate.
AWS Prescriptive Guidance	Migration strategies, guides, and patterns.

1.4 Cloud economics

Concept	Explanation
Fixed vs. variable cost	On-premises involves upfront fixed cost (hardware, data center). In the cloud the cost is variable and proportional to usage.
On-premises associated costs	Servers and hardware, space, power and cooling, operations and maintenance staff, and licenses.
Licensing	**BYOL** (bring your own license) vs. **license included** in the service price. AWS License Manager helps manage licenses; Dedicated Hosts allow the use of server-bound licenses.
Rightsizing	Match the size of resources to the actual load. AWS Compute Optimizer and AWS Cost Explorer support the analysis.
Automation	Infrastructure as code (AWS CloudFormation) reduces manual effort and human error; repeatable and fast processes.
Economies of scale	The aggregated volume of customers lowers the price per unit for everyone.

> **Trap:** cloud economics are not automatic: they come from paying only for usage, rightsizing, turning off idle resources, and suitable purchase options.

1.5 Architecture concepts the exam covers

Concept	Definition
Vertical scaling (scale up)	A larger instance (more CPU/RAM). Has a ceiling and usually requires downtime to resize.
Horizontal scaling (scale out)	More instances. No hard ceiling; pairs well with load balancers and cloud elasticity.
Elasticity	Grow **and shrink** automatically according to demand; it is the property typically associated with the "cloud".
High availability (HA)	Minimize downtime, normally with redundant resources across multiple AZs.
Fault tolerance	The system keeps working correctly even when a component fails; a stronger guarantee than HA.
RTO (Recovery Time Objective)	Maximum acceptable time to restore the service (how long I can be down).
RPO (Recovery Point Objective)	Maximum acceptable data loss, measured in time since the last backup.
Loose coupling	Components communicate through well-defined interfaces (queues, APIs), so the failure of one does not propagate. Services: SQS, SNS, EventBridge.
Microservices vs. monolith	Microservices: application split into small, independently deployable services. Monolith: one large, tightly coupled application.

Question patterns: "migrate as fast as possible, with minimal changes" → **Rehost**. "Take advantage of cloud-native scalability in the long term, investing engineering effort" → **Refactor**. "Migrate gradually by connecting the data center to AWS" → **hybrid cloud** (Direct Connect, Site-to-Site VPN, Storage Gateway, Outposts). "No longer have to predict capacity" → **stop guessing capacity**. "Move from upfront investment to ongoing spending" → **CapEx to OpEx**.

Trap: "use resources efficiently and adapt to demand" is **Performance Efficiency**, not Cost Optimization; cost is specifically the price dimension.

📋 Quick Summary of Domain 1

- 6 advantages: variable expense, economies of scale, stop guessing capacity, speed and agility, no data center costs, global reach.
- High availability = multiple AZs. Elasticity = scale up and down according to demand.
- Well-Architected: Operational Excellence, Security, Reliability, Performance Efficiency, Cost Optimization, Sustainability. The Tool is free.
- CAF: Business, People, Governance, Platform, Security, Operations. Phases: Envision, Align, Launch, Scale.
- 7 Rs: Retire, Retain, Rehost, Relocate, Repurchase, Replatform, Refactor.
- DMS = databases · Application Migration Service = servers · Migration Hub = tracking · Discovery Service = inventory.

> **Traps:** (1) Rehost does not optimize, it only moves. (2) Relocate does not require rewriting applications. (3) Refactor is the most complex and costly.

Domain 2: Security and Compliance (30%)

Official task statements: 2.1 shared responsibility model · 2.2 security, governance, and compliance concepts · 2.3 access management · 2.4 security components and resources.

2.1 Shared responsibility model

	AWS: security *of* the cloud	**Customer: security *in* the cloud**
Scope	Hardware, software, network, and facilities that run AWS services.	Data, applications, and configuration appropriate to the chosen service.
Examples	Data centers, hardware, global infrastructure, hypervisor.	Data, IAM, firewall/security groups, encryption, guest OS and patches (on EC2).

Control type	**Description**	**Examples**
Inherited	Fully managed by AWS.	Physical and environmental security
Shared	Both contribute, each within their own scope.	Patch management, configuration management, awareness and training
Customer specific	Depend on the customer's deployment.	Data routing, zone security

How responsibility changes depending on the service

Service	**AWS takes care of**	**You take care of**
Amazon EC2 (IaaS)	Hardware and infrastructure	Guest OS, patches, applications, security groups, data
Amazon RDS (managed)	Hardware, host OS, engine installation and patching, automated backups	Data, access control, network configuration, and encryption
AWS Lambda (serverless)	Infrastructure, OS, and runtime	Your code, IAM permissions, and data
Amazon S3 / DynamoDB	Infrastructure operation	Data classification and IAM permissions

> **Trap:** the more managed the service, the smaller the customer's responsibility; but data and access are **always** the customer's.

2.2 Security, governance, and compliance

Compliance

- **AWS Artifact:** self-service portal to download AWS compliance reports and accept agreements. It is where to find compliance information.
- Compliance requirements vary by **geographic location**, **industry**, and **service**; consult the AWS Compliance page.

Encryption

Type	Protects	Tools
In transit	Data moving across the network (TLS/HTTPS)	AWS Certificate Manager (ACM), VPN
At rest	Stored data	AWS KMS (keys), AWS CloudHSM (dedicated HSM), native encryption for S3, EBS, RDS

Monitoring, auditing, and logs

Service	Function	Question it answers
Amazon CloudWatch	Monitoring: metrics, logs, and alarms	How is performance?
AWS CloudTrail	Records API calls and activity in the account	Who did what, and when?
AWS Config	Assesses and records resource configurations and compliance	How is the resource configured and what changed?
Access reports	IAM credential report and last accessed information	Which credentials and permissions are unused?

Services to protect resources

Service	What it is for
Amazon GuardDuty	Intelligent threat detection for accounts and workloads.
Amazon Inspector	Automated vulnerability scanning (e.g., EC2, container images, Lambda).
AWS Security Hub	Centralized view of security alerts and findings and compliance checks.
AWS Shield	DDoS protection. **Standard**: automatic, free, for all customers. **Advanced**: paid, more sophisticated detection and mitigation, 24/7 access to the DDoS response team, and cost protection.
AWS WAF	Web application firewall: protects against common web exploits.
AWS Firewall Manager	Centrally manage firewall rules (e.g., WAF) across multiple accounts through AWS Organizations.
Amazon Macie	Discover and protect sensitive data, such as PII, in Amazon S3.
Amazon Detective	Investigate the root cause of security findings.
AWS KMS	Create and control encryption keys.
AWS CloudHSM	Dedicated hardware security module.
AWS Secrets Manager	Store and rotate secrets (passwords, API keys).
AWS Certificate Manager	Provision and manage SSL/TLS certificates.
AWS Resource Access Manager	Share resources across accounts securely.
Amazon Cognito	Identity and access for customers of web and mobile applications.
AWS Directory Service	Managed Microsoft Active Directory.
AWS Audit Manager	Continuously audit AWS usage to simplify risk and compliance assessment (cited in study material; not on the official exam service list).

2.3 Access management

Concept	Description
AWS IAM	Controls who (authentication) can do what (authorization) on resources.
Users, groups, roles	User = identity of a person or application; group = a set of users; role = identity with temporary credentials, assumed by people, services, or other accounts.
Policies	JSON documents that define permissions. **AWS managed** (ready-made) or **customer managed** (custom); inline policies also exist.
Least privilege	Grant only the permissions needed for the task.
MFA	Second authentication factor; recommended for root and IAM users.
IAM Identity Center	Centralized workforce access management across multiple accounts and applications (federated identity).
Cross-account roles	IAM roles allow access between accounts (cross-account).
Access keys	Long-term credentials; prefer temporary credentials via roles and rotate keys when needed.
Storing credentials	AWS Secrets Manager and AWS Systems Manager (Parameter Store).

Root user

- Initial identity with full access to the account. **Do not use it for everyday tasks**; use an administrative user in IAM Identity Center.
- Protect it with **MFA**, a strong password, and remove root access keys when they are not needed.
- **Tasks that require the root user** (official list, excerpts): change account settings (email, password) in standalone accounts; close the account; reopen the account; restore IAM permissions when the only administrator revoked their own; activate IAM access to the Billing console; sign up for AWS GovCloud (US); register as a seller in the EC2 Reserved Instance Marketplace; configure MFA delete on an S3 bucket; edit or delete an S3 bucket policy or SQS queue policy that denies all principals.

Official IAM best practices

- Require federation with an identity provider and temporary credentials for people.
- Require workloads to use IAM roles (temporary credentials).
- Require MFA (prefer phishing-resistant MFA, such as passkeys and security keys).
- Apply least-privilege permissions; start with AWS managed policies and evolve to customer managed ones.
- Use IAM Access Analyzer to validate policies and check for public or cross-account access.
- Review and remove unused users, roles, permissions, and credentials.
- Use AWS Organizations SCPs as guardrails (they do not grant permissions) and permissions boundaries to delegate.

2.4 Security components and resources

- **Third-party:** third-party security products are available in **AWS Marketplace**.

- **Where to find information:** AWS Knowledge Center, AWS Security Center, and AWS Security Blog.
- **AWS Trusted Advisor:** checks the environment and recommends actions in cost, performance, security, resilience, operational excellence, and service limits. (Older study material cites 5 categories: cost, performance, security, fault tolerance, and service limits.)

2.5 Network security and summary tables

	Security Group	Network ACL (NACL)
Level	Instance (EC2/ENI)	Subnet
State	**Stateful**: return traffic is automatically allowed	**Stateless**: inbound and outbound rules must be defined
Rule types	Allow only	Allow and deny
Evaluation	All rules are evaluated	In numerical order; the first match applies

Component	Function
Subnets, route tables, Internet Gateway	A public subnet has a route to the internet through the Internet Gateway.
NAT Gateway	Allows outbound internet access from private subnets, without allowing inbound.
VPC Peering	Direct connection between two VPCs.
VPC Endpoints	Private access from the VPC to AWS services without going over the public internet.

Which service to use? (trigger table)

Need	Answer
Temporary access from one AWS service to another (e.g., EC2 accessing S3)	**IAM Role** (never fixed keys on the instance)
Someone from another account needs to access your resources	Cross-account IAM role
Centralized login across multiple accounts	IAM Identity Center
Extra security at login	MFA
Least privilege for a new employee	Custom IAM policy attached to a group
Is the configuration compliant? What changed?	AWS Config
Who made which API call and when?	AWS CloudTrail
Sensitive data/PII in S3	Amazon Macie
Compromised instance or malicious activity	Amazon GuardDuty (analyzes CloudTrail, VPC Flow Logs, and DNS logs)
Vulnerabilities (CVEs) in EC2, containers, Lambda	Amazon Inspector
Single pane for security findings	AWS Security Hub
SQL injection and XSS in the web application	AWS WAF (layer 7; CloudFront, ALB, API Gateway)
DDoS	AWS Shield
WAF/security group rules across multiple accounts	AWS Firewall Manager
AWS compliance certificates (SOC, PCI-DSS, ISO) and agreements (e.g., BAA)	AWS Artifact
Store and rotate a database password	AWS Secrets Manager
Manage encryption keys	AWS KMS (AWS managed or customer managed keys)
Free SSL/TLS certificate for the load balancer	AWS Certificate Manager
Best practice checks on cost/security/performance	AWS Trusted Advisor

> **Config vs. CloudTrail** is the most confused pair in the domain: **Config** = how the resource is and how it changed; **CloudTrail** = who did what, when, and from where.

📋 Quick Summary of Domain 2

- AWS = security *of* the cloud. Customer = security *in* the cloud.
- Patching, configuration, and training = shared controls.
- AWS Artifact = compliance reports. CloudTrail = who called the API. CloudWatch = metrics and logs. Config = configuration and compliance.
- GuardDuty = threats · Inspector = vulnerabilities · Macie = sensitive data in S3 · Shield = DDoS · WAF = web attacks · Security Hub = central view.
- KMS = keys · CloudHSM = dedicated HSM · Secrets Manager = secrets · ACM = certificates.
- Root: MFA and minimal use. Day to day: IAM Identity Center. Least privilege always.

> **Traps:** (1) Data and IAM are always the customer's. (2) CloudTrail (API auditing) is not the same as CloudWatch (monitoring). (3) SCPs do not grant permissions.

Domain 3: Cloud Technology and Services (34%)

Official task statements: 3.1 deploy and operate · 3.2 global infrastructure · 3.3 compute · 3.4 databases · 3.5 networking · 3.6 storage · 3.7 AI/ML and data analytics · 3.8 other categories.

3.1 Deployment and Operation Methods

Method	When to use
AWS Management Console	Web interface; ideal for one-off operations and exploration.
AWS CLI	Command line; automation and scripts.
SDKs and APIs	Programmatic access from application code.
Infrastructure as code (IaC)	**Repeatable**, versioned processes (e.g., AWS CloudFormation).

> **One-off** operation → Console. **Repeatable** process → CLI/SDK/IaC. Deployment models: **cloud**, **hybrid**, **on-premises**.

3.2 AWS Global Infrastructure

Component	Definition
Region	Physical location where AWS clusters data centers; each Region has a **minimum of three** isolated and physically separated AZs.
Availability Zone (AZ)	One or more discrete data centers with redundant power, networking, and connectivity; AZs are many kilometers apart from each other, within 100 km, connected by a low-latency network.
Edge locations	Points of presence used to deliver content with low latency (e.g., Amazon CloudFront).
Local Zones	Extensions of a Region that place compute and storage closer to users (single-digit millisecond latency).
AWS Wavelength	Infrastructure embedded in telecom providers' 5G networks for ultra-low-latency applications.

- **High availability:** distribute the load across **multiple AZs**; AZs do not share single points of failure.
- **When to use multiple Regions:** disaster recovery, business continuity, low latency for end users, and **data sovereignty**.
- At the time of consulting the official page: 39 Regions and 124 AZs (the numbers change over time).

3.3 Compute Services

EC2 instance family	Use
General purpose	Balance of compute, memory, and networking (web servers, databases).
Compute optimized	Compute-intensive applications (batch processing, media transcoding, game servers).
Memory optimized	Large datasets in RAM (in-memory databases, analytics).
Accelerated computing	Hardware accelerators (graphics, ML).
Storage optimized	Millions of low-latency random I/O operations (high-throughput databases).
HPC optimized	Best price performance for HPC workloads at scale.

Service	Description
Amazon EC2	Secure, resizable compute capacity (virtual servers).
EC2 Auto Scaling	Adds or removes instances based on defined conditions: provides **elasticity**.
Elastic Load Balancing	Distributes traffic across multiple targets. **ALB**: HTTP/HTTPS (layer 7). **NLB**: TCP, extreme performance (layer 4). **GWLB**: third-party appliances.
AWS Lambda	Runs code without managing servers; pay only for compute time.
AWS Fargate	Serverless engine for containers (ECS and EKS), without managing servers.
Amazon ECS	Container orchestration, simple and AWS-native. **Amazon EKS**: managed Kubernetes (when you specifically need Kubernetes or a portable strategy). **Amazon ECR**: image registry.
AWS Elastic Beanstalk	You upload the code; the service handles provisioning, load balancing, scaling, and monitoring.
Amazon Lightsail	Simple virtual private server, with low and predictable pricing.
AWS Batch	Batch processing at any scale.
AWS Outposts	AWS infrastructure and services in your own data center (hybrid).

3.4 Database Services

Type	Service	Official note
Relational	**Amazon RDS**	Sets up, operates, and scales relational databases; automates provisioning, patching, and backups.
Relational	**Amazon Aurora**	Compatible with MySQL and PostgreSQL; replication across three AZs; managed by RDS.
Key-value / NoSQL	**Amazon DynamoDB**	Key-value and document; single-digit millisecond performance at any scale.
In-memory	**Amazon ElastiCache**	In-memory cache (Redis OSS and Memcached) to speed up applications.
Document	**Amazon DocumentDB**	MongoDB compatible.
Graph	**Amazon Neptune**	Highly connected data: fraud detection, recommendations.
Data warehouse	**Amazon Redshift**	Analytical data warehousing with SQL.

- **EC2 vs. managed database:** on EC2 you administer everything (OS, patches, backups); with managed services AWS takes over those tasks.
- **Migration:** AWS DMS (migration and replication) and AWS SCT (schema conversion).

3.5 Networking Services

Service / component	Description
Amazon VPC	Logically isolated section of the cloud, with control over the IP range, subnets, route tables, and gateways.
Public vs. private subnet	Public has internet access; private hosts backends without direct internet access.
Security groups	Instance-level firewall (allow traffic; **stateful**).
Network ACLs	Subnet-level firewall (**stateless**, allow and deny rules).
Amazon Route 53	Highly available and scalable DNS; latency-based, geolocation, weighted, and failover routing; domain registration.
Amazon CloudFront	CDN that delivers content globally with low latency.
AWS Direct Connect	**Dedicated** network connection between your location and AWS.
AWS Site-to-Site VPN / Client VPN	Encrypted tunnels between networks and AWS; Client VPN for remote users.
AWS Transit Gateway	Central hub that connects VPCs and on-premises networks (hub-and-spoke model).
AWS PrivateLink	Private connectivity between VPCs, AWS services, and on-premises applications, without exposing them to the internet.
AWS Global Accelerator	Uses the AWS global network and static IPs to improve availability and performance.
Amazon API Gateway	Creates, publishes, and secures APIs at any scale.

> **Trap:** Direct Connect = dedicated, private connection; VPN = encrypted tunnel over the internet. Amazon Inspector is not a firewall; network security in the VPC is done with security groups and NACLs.

3.6 Storage Services

Type	Service	Description
Object	**Amazon S3**	Scalability, availability, and durability of 99.999999999% (11 nines).
Block	**Amazon EBS**	Persistent volumes for EC2, replicated within the AZ. **Instance store**: temporary storage local to the instance.
File	**Amazon EFS**	Elastic file system for Linux, shared by thousands of instances.
File	**Amazon FSx**	Managed file systems (Windows File Server, Lustre, NetApp ONTAP, OpenZFS).
Hybrid	**AWS Storage Gateway**	On-premises applications use AWS storage, with local caching.
Protection	**AWS Backup**	Centralizes and automates backups across multiple services (policies, Organizations integration).
Recovery	**AWS Elastic Disaster Recovery**	Fast recovery of on-premises and cloud applications.

Amazon S3 Storage Classes

Class	Use
S3 Standard	Frequently accessed data.
S3 Intelligent-Tiering	Unknown or changing access pattern; moves objects between tiers automatically.
S3 Express One Zone	High-performance access, single-digit millisecond latency, in one AZ.
S3 Standard-IA	Infrequent access; multiple AZs.
S3 One Zone-IA	Infrequent access; a single AZ (costs less).
S3 Glacier Instant Retrieval	Archive accessed a few times per year, with immediate retrieval.
S3 Glacier Flexible Retrieval	Backup and archive; retrieval from minutes to hours.
S3 Glacier Deep Archive	Lowest cost; retrieval in 12 to 48 hours; long-term retention.

- **Lifecycle policies:** automatically move objects between classes (or expire them) without changing the application.
- S3 Object Lock: WORM storage (write once, read many).

3.7 AI/ML and Data Analytics

Service	What it does
Amazon SageMaker AI	Build, train, and deploy ML models.
Amazon Lex	Conversational chatbots (voice and text).
Amazon Comprehend	Natural language processing: sentiment, entities, key phrases.
Amazon Rekognition	Image and video analysis.
Amazon Textract	Extraction of text and data from documents.
Amazon Transcribe	Speech to text.
Amazon Polly	Text to speech.
Amazon Translate	Language translation.
Amazon Q	Generative AI assistant.

Analytics service	Official description
Amazon Athena	Interactive SQL queries on data in S3; serverless, pay per query.
Amazon Kinesis	Collect, process, and analyze streaming data in real time.
AWS Glue	Fully managed ETL service; maintains the Data Catalog.
Amazon Quick	Cloud business intelligence: interactive dashboards.
Amazon EMR	Big data platform with Spark, Hive, Presto, and others.
Amazon Redshift	Cloud data warehouse.
Amazon OpenSearch Service	Search, log analytics, and visualization.

3.8 Other Service Categories

Category	Services and function
Application integration	**Amazon SQS**: queues (decouples; standard = best-effort ordering, FIFO = guaranteed ordering). **Amazon SNS**: pub/sub, push notifications, email, and SMS. **Amazon EventBridge**: serverless event bus. **AWS Step Functions**: visual workflows.
Business applications	**Amazon Connect**: contact center. **Amazon SES**: email sending.
Developer tools	**AWS CodeBuild**: builds and tests. **AWS CodePipeline**: continuous delivery pipeline. **AWS X-Ray**: traces and debugs applications. **AWS CLI**.
End-user computing	**Amazon AppStream 2.0**: streams applications. **Amazon WorkSpaces**: virtual desktops. **WorkSpaces Secure Browser**: secure browser.
Frontend web and mobile	**AWS Amplify**: build and deploy web and mobile apps.
IoT	**AWS IoT Core**: connect and manage IoT devices.
Customer support	**AWS Support**: technical assistance options (see Domain 4).

3.9 Comparisons and Exam Tips

Pair	Difference
CloudFormation vs. Elastic Beanstalk	CloudFormation: defines each resource in JSON/YAML templates (full control, repeatable, versionable, "stack"). Beanstalk: upload the code and it provisions everything (less control, faster). AWS CDK: IaC in programming languages, generates CloudFormation (not in the official list).
CloudFront vs. Global Accelerator	CloudFront: edge caching, ideal for static/cacheable content. Global Accelerator: routes traffic over the AWS network, ideal for dynamic traffic, TCP/UDP (gaming, VoIP).
SQS vs. SNS	SQS: queue, pull, one message consumed by one consumer. SNS: topic, push, fan-out to multiple subscribers (email, SMS, Lambda, SQS).
EBS vs. EFS vs. S3	EBS: block, one instance at a time (virtual disk). EFS: file (NFS), multiple instances at the same time. S3: object, via API, no "mounting" on the server.
RDS/Aurora vs. DynamoDB	Relational/SQL/structured vs. NoSQL, massive scale, flexible schema.
Direct Connect vs. VPN	Dedicated private line, consistent bandwidth vs. encrypted tunnel over the internet, faster to set up.

- **Spot:** can be interrupted with a 2-minute notice; never for critical or stateful workloads.
- **S3 features:** versioning (protects against accidental deletion/overwrite), lifecycle policies, cross-Region or same-Region replication, encryption, and Block Public Access.
- **AWS Snow Family** (Snowcone, Snowball, Snowmobile): physical transfer of large volumes of data when there is little or no bandwidth.

- **AWS Systems Manager:** operations hub: patching, commands across fleets, Parameter Store, Session Manager (shell without SSH).
- **AWS Organizations:** manages multiple accounts, with consolidated billing and **SCPs** (maximum permissions limit; they are guardrails, they do not grant permissions). **AWS Control Tower** creates a multi-account environment (landing zone) with best practices.
- **CI/CD:** CodeBuild (builds) and CodePipeline (orchestrates) are in the official scope; CodeCommit and CodeDeploy appear in study material, but are not in the current official list.
- **Outside the official list, but mentioned in study material:** Amazon Kendra (enterprise search) and Amazon Bedrock (foundation models via API).

📋 Domain 3 Quick Summary

- Region ≥ 3 AZs. High availability = multiple AZs. Multiple Regions = DR, low latency, data sovereignty.
- EC2 (VMs), Lambda (serverless), Fargate (serverless containers), ECS/EKS (containers), Beanstalk (PaaS), Lightsail (simple), Outposts (hybrid).
- RDS/Aurora = relational · DynamoDB = NoSQL · ElastiCache = memory · Neptune = graph · DocumentDB = document · Redshift = data warehouse.
- Security group = instance (stateful). NACL = subnet (stateless). Direct Connect = dedicated. VPN = encrypted over the internet.
- S3 = object · EBS = block · EFS/FSx = file · Storage Gateway = hybrid · Backup = centralized backups.
- Athena = SQL on S3 · Glue = ETL · Kinesis = streaming · Quick = BI · SageMaker AI = ML · Lex = chatbot.
- SQS = queue · SNS = notification · EventBridge = events.

> **Traps:** (1) EBS is block; EFS is file; S3 is object. (2) Aurora is managed by RDS. (3) Glacier Deep Archive takes hours to retrieve.

Domain 4: Billing, Pricing, and Support (12%)

Official task statements: 4.1 pricing models · 4.2 billing, budgeting, and cost management · 4.3 technical resources and support plans.

4.1 Pricing models

Official principles: **pay as you go**; **save when you commit** (Savings Plans, in USD/hour for 1 or 3 years); **pay less by using more** (tiered pricing by volume).

Purchase option	Description	When to use
On-Demand	Pay by the hour or second, with no commitment or upfront payment.	Short, unpredictable workloads that cannot be interrupted; first tests.
Savings Plans	Lower price (up to 72%) in exchange for a commitment to consistent usage (USD/hour) for 1 or 3 years.	Steady and flexible usage.
Reserved Instances	Discount of up to 72% compared to On-Demand. Convertible RIs let you change family, OS, and tenancy.	Predictable, continuous usage.
Spot Instances	Spare capacity at up to 90% discount.	Fault-tolerant workloads with flexible start and end times.
Dedicated Hosts	Physical server dedicated to you; allows server-bound licenses (e.g., Windows Server, SQL Server).	Licensing and compliance.
Dedicated Instances	Instances on hardware dedicated to a single customer.	Hardware isolation.
Capacity Reservations	Capacity reservation for guaranteed availability during critical events or disaster recovery.	Guarantee capacity.

- **Reserved Instances in AWS Organizations:** with consolidated billing, RI and Savings Plans discounts can be shared across accounts.
- **Per-second billing** (60-second minimum) for EC2 instances.

Data transfer and storage

- Data transfer **in (IN) is free**; data transfer **out (OUT)** is charged in tiers, with a lower price as volume increases.
- Transfer between Regions has a cost; storage pricing varies by service and by tier/class (e.g., S3 classes).
- The Free Tier lets you try out services.

4.2 Billing, budgeting, and cost management

Tool	Function
AWS Pricing Calculator	Estimates the cost of an architecture **before** you deploy it.
AWS Cost Explorer	Visualizes, understands, and manages costs and usage over time; supports forecasting.
AWS Budgets	Sets thresholds and sends alerts when actual or forecasted spend exceeds the budget.
AWS Cost and Usage Report	Detailed cost and usage data, the most comprehensive.
AWS Billing Conductor	Cost allocation strategy aligned with business logic.
AWS Compute Optimizer	Recommendations for compute rightsizing.

AWS Organizations and consolidated billing

- There is one **management** account that pays the charges of all member accounts.
- Benefits: **a single bill**, easy tracking, **combined usage** (shared volume, RI, and Savings Plans discounts), and **no additional cost**.

Cost allocation tags

- Key-value labels applied to resources. Two types: **AWS-generated** (prefix `aws:`) and **user-defined** (prefix `user:`).
- They must be **activated** in the Billing console and can take up to 24 hours to appear; they become available in Cost Explorer and in reports (e.g., Cost and Usage Report).

4.3 Technical resources and support plans

Plan	Highlights (official plans page)
Basic Support	Included for everyone: 24/7 customer service, documentation, whitepapers, AWS re:Post, core Trusted Advisor checks, and AWS Health.
Business Support+	Recommended minimum for production workloads: response in under 30 min (business-critical system down) and 1 hour (production system down); 24/7 support by phone, web, chat, and email; account and billing support; full Trusted Advisor checks.
Enterprise Support	Critical workloads: response in under 15 min; designated **Technical Account Manager (TAM)**; customized strategic plan; proactive security reviews.
Unified Operations	Mission-critical workloads: response in under 5 min by an Incident Management Engineer; Domain Specialist Engineers; ongoing architectural reviews.

> **AWS Trusted Advisor** recommends actions in six areas: cost optimization, performance, security, resilience, operational excellence, and service limits. All accounts get 56 core checks; Business Support+ or higher unlocks the expanded set (482 checks, according to the official page), with API and CLI access.

Resource	What it is for
AWS Health Dashboard / AWS Health API	Health events for services and for your account; monitor and manage your environment.
AWS Knowledge Center, AWS re:Post, AWS Prescriptive Guidance	Frequently asked questions, community, and technical guidance.
Whitepapers, blogs, and documentation	Official material on AWS websites.
AWS Support Center	Open and track support cases.
AWS Trust and Safety	Report abuse of AWS resources.
AWS Professional Services and solutions architects	Technical assistance from AWS.
AWS Partner Network (APN)	Partners, including ISVs and system integrators; benefits such as training and certification, events, and volume discounts.
AWS Marketplace	Digital catalog of third-party software, with cost management tools, governance, and entitlements.

Free Tier and other items

- **Always Free:** free forever up to a limit (e.g., first million Lambda requests per month).
- **12 months free:** from account creation, up to usage limits.
- **Trials:** short-term trials starting from service activation (varies by service).
- **AWS Marketplace:** third-party software (AMIs, SaaS, data) deployed in your account and billed on your AWS bill.
- **Migration Evaluator:** builds the business case and cost estimate for migration; **Application Discovery Service** collects data from on-premises servers.
- **Cost Explorer recommendations** show where committing (RIs/Savings Plans) would save money, based on usage history.

> **Heads up: older plan names:** older study materials mention the **Developer**, **Business**, and **Enterprise On-Ramp** plans. The current official page and the exam guide list Basic, Business Support+, Enterprise Support, and Unified Operations. If a practice exam uses the old names, treat them as a previous version. In any version, only Basic is free and the TAM only comes with Enterprise-level plans.

📋 Quick Summary of Domain 4

- On-Demand = flexible · Savings Plans/RIs = commitment (up to 72%) · Spot = up to 90%, can be interrupted · Dedicated Hosts = licenses and compliance.
- Data IN is free; data OUT is charged in tiers.
- Pricing Calculator = estimate beforehand · Cost Explorer = analyze the past and forecast · Budgets = alerts · CUR = detailed report.
- Organizations = single bill and combined discounts, at no cost. Tags must be activated.
- Plans: Basic, Business Support+, Enterprise Support, Unified Operations. TAM with Enterprise Support.
- Trusted Advisor = recommendations; Health Dashboard = service events.

> **Traps:** (1) Spot can be interrupted. (2) Pricing Calculator estimates; Cost Explorer analyzes actual spend. (3) Tags do not appear without activation.

Final Review

Contrast table (last-minute review)

Easily confused pair	Distinction
Scalability vs. Elasticity	Scalability: can grow. Elasticity: grows and shrinks automatically.
HA vs. Fault tolerance	HA: minimizes downtime with redundancy. Fault tolerance: keeps working during the failure.
RTO vs. RPO	RTO: time to recover. RPO: acceptable data loss (time since the last backup).
Vertical vs. Horizontal	Vertical: larger instance, with a ceiling. Horizontal: more instances, no hard ceiling.
Security Group vs. NACL	Instance, stateful, allow only vs. subnet, stateless, allow and deny, in order.
Config vs. CloudTrail	Configuration/compliance vs. who called which API.
CloudFront vs. Global Accelerator	Edge caching vs. optimized routing of dynamic traffic.
SQS vs. SNS	Queue, pull, one consumer vs. topic, push, multiple subscribers.
EBS vs. EFS vs. S3	Block vs. shared file vs. object.
Direct Connect vs. VPN	Dedicated and private vs. encrypted over the internet.
CapEx vs. OpEx	Upfront investment vs. pay-as-you-use spending.
RIs vs. Savings Plans	Commitment to a specific instance vs. commitment in USD/hour, more flexible.
Cost Explorer vs. Pricing Calculator	Actual past spend vs. future estimate.
IAM Role vs. IAM User	Temporary, assumed vs. persistent identity.
GuardDuty vs. Inspector vs. Security Hub	Threats from logs vs. vulnerabilities/CVEs vs. aggregated dashboard.

Traps that cost points

1. "AWS takes care of that automatically" is wrong for IAM design, choice of encryption keys, security group rules, and OS patches on EC2.
2. Security Group vs. NACL: read "instance" vs. "subnet" and "stateful" vs. "rules in both directions".
3. Spot is never the answer for a workload that cannot tolerate interruption or is critical/stateful.
4. CloudFront (static/cacheable) vs. Global Accelerator (dynamic, gaming, VoIP).
5. Config vs. CloudTrail: "how the resource is" vs. "who called which API".
6. Support plans: only Basic is free; do not mix up the response times (Business Support+ vs. Enterprise Support).
7. RTO is time; RPO is data. Do not swap them.

8. The "fastest and cheapest to start" migration is Rehost, not Refactor.
9. SCPs are guardrails, not grants of permissions; the account IAM policies still need to allow the action.
10. "How to reduce costs" has several possible answers: combine the keyword (steady usage, interruptible, aging data) with the tool (RI/Savings Plans, Spot, S3 lifecycle).

Self-test: explain out loud

1. What is the difference between elasticity and scalability?
2. Why is the security group stateful and the NACL not? What does that change for the response packet?
3. Give one scenario where Spot is ideal and another where it is dangerous.
4. What does AWS Config record and what does CloudTrail record?
5. In the shared responsibility model, name three things that remain the customer's responsibility even on RDS.
6. Why choose Global Accelerator instead of CloudFront for a real-time multiplayer game?
7. What is the difference between RTO and RPO, and how does each appear in a disaster recovery requirement?
8. When should you choose DynamoDB instead of RDS?
9. What is the difference between SQS and SNS in one sentence?
10. Which support plan includes a Technical Account Manager, and what does the TAM do that a regular case does not?

Sources

Content consulted on **2026-11-21**, from public pages of the **official AWS website** (aws.amazon.com and docs.aws.amazon.com):

- Official CLF-C02 exam guide: https://docs.aws.amazon.com/aws-certification/latest/cloud-practitioner-02/cloud-practitioner-02.html
- Domain 1: https://docs.aws.amazon.com/aws-certification/latest/cloud-practitioner-02/cloud-practitioner-02-domain1.html
- Domain 2: https://docs.aws.amazon.com/aws-certification/latest/cloud-practitioner-02/cloud-practitioner-02-domain2.html
- Domain 3: https://docs.aws.amazon.com/aws-certification/latest/cloud-practitioner-02/cloud-practitioner-02-domain3.html
- Domain 4: https://docs.aws.amazon.com/aws-certification/latest/cloud-practitioner-02/cloud-practitioner-02-domain4.html
- In-scope services: https://docs.aws.amazon.com/aws-certification/latest/cloud-practitioner-02/clf-02-in-scope-services.html
- Technologies and concepts: https://docs.aws.amazon.com/aws-certification/latest/cloud-practitioner-02/clf-technologies-concepts.html
- Certification page: https://aws.amazon.com/certification/certified-cloud-practitioner/
- Six advantages of cloud computing (Overview of AWS): https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html
- AWS Well-Architected: https://aws.amazon.com/architecture/well-architected/
- AWS CAF: overview and journey: https://docs.aws.amazon.com/whitepapers/latest/overview-aws-cloud-adoption-framework/welcome.html
- AWS CAF: foundational capabilities: https://docs.aws.amazon.com/whitepapers/latest/overview-aws-cloud-adoption-framework/foundational-capabilities.html
- Migration strategies (7 Rs): https://docs.aws.amazon.com/prescriptive-guidance/latest/large-migration-guide/migration-strategies.html
- Shared responsibility model: https://aws.amazon.com/compliance/shared-responsibility-model/
- IAM: root user and tasks that require root: https://docs.aws.amazon.com/IAM/latest/UserGuide/root-user-tasks.html
- IAM: security best practices: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html
- Security, identity, and compliance: https://aws.amazon.com/products/security/
- Global infrastructure: Regions and AZs: https://aws.amazon.com/about-aws/global-infrastructure/regions_az/
- EC2 instance types: https://aws.amazon.com/ec2/instance-types/
- EC2 pricing: https://aws.amazon.com/ec2/pricing/
- S3 storage classes: https://aws.amazon.com/s3/storage-classes/
- Overview of AWS: Compute: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/compute-services.html

- Overview of AWS: Databases: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/database.html
- Overview of AWS: Networking: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/networking-services.html
- Overview of AWS: Storage: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/storage-services.html
- Overview of AWS: Management and governance: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/management-and-governance.html
- Overview of AWS: Analytics: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/analytics.html
- Overview of AWS: Application integration: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/application-integration.html
- AWS Support plans: https://aws.amazon.com/premiumsupport/plans/
- AWS Trusted Advisor: https://aws.amazon.com/premiumsupport/technology/trusted-advisor/
- AWS pricing: https://aws.amazon.com/pricing/
- Cloud financial management: https://aws.amazon.com/aws-cost-management/
- Consolidated billing: https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html
- Cost allocation tags: https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/cost-alloc-tags.html

> **Transparency: AWS Skill Builder** requires a login and was not accessed directly, so please cross-check the content there. Some short service descriptions (for example security and AI/ML) and details such as security groups vs. NACLs were written from standard AWS documentation, and some pages consulted had little detail. Numbers such as Region count, maximum discounts and number of Trusted Advisor checks change over time: confirm them on the pages before the exam.