CLF-C02 Cloud Practitioner Free Sample (30 Questions)

Unofficial practice material. Not affiliated with or endorsed by Amazon.

This free sample contains 30 of the 865 questions from the full CLF-C02 Cloud Practitioner question bank.

Q1. A team focuses on running and monitoring systems, delivering business value, and continually improving their processes and procedures. Which Well-Architected pillar does this describe?

A) Reliability

B) Operational excellence

C) Performance efficiency

D) Security

Correct answer: B

Explanation: Operational excellence is about running and monitoring systems to deliver business value and continuously improving processes and procedures, including using runbooks and learning from failures. Why the others are wrong - A: Reliability focuses on recovering from failures and meeting demand, not on day-to-day operational processes.; C: Performance efficiency is about using compute resources efficiently and maintaining that efficiency as demand changes.; D: Security focuses on protecting information, systems, and assets.

Q2. A company is preparing a total cost of ownership (TCO) comparison between its data center and AWS. Which set of on-premises costs MUST be included for a fair comparison?

A) Only the purchase price of the servers

B) Only the salaries of the application developers

C) Hardware, facilities, power and cooling, and the IT labor required to run the data center

D) Only hardware and power costs, since staff time for running the data center is already paid for.

Correct answer: C

Explanation: A realistic on-premises TCO must include hardware AND the facilities, power, cooling, and personnel costs of running a data center; ignoring them understates the true cost of staying on premises. Why the others are wrong - A: Server price alone ignores facilities and operational costs, making the comparison misleading.; B: Developer salaries are not a hosting cost differentiator here; data center operations labor is the relevant item.; D: The IT labor required to operate a data center is a major ongoing cost of ownership; excluding it makes the TCO comparison unfair.

Q3. A company tags every resource by project so it can see exactly which team spends what, and reviews the return on that spending monthly. Which cost optimization principle is this?

A) Maintain traceability

B) Test recovery procedures

C) Analyze and attribute expenditure

D) Prepare for security events

Correct answer: C

Explanation: Analyze and attribute expenditure is a cost optimization principle: identify and attribute the usage and cost of each workload so teams can measure return on investment and optimize spending. Why the others are wrong - A: Traceability is the security principle of monitoring and auditing actions - related to visibility, but about security events, not spend attribution.; B: Testing recovery procedures is a reliability principle.; D: Preparing for security events (incident response readiness) belongs to the security pillar.

Q4. A company regularly runs exercises in which it deliberately terminates random production servers to confirm that traffic automatically shifts to healthy ones. Which pillar's principles are being applied?

A) Security, because the exercise validates access controls

B) Cost optimization, because terminated servers stop incurring charges

C) Reliability, because the exercise tests the workload's ability to recover from failures automatically

D) Operational excellence, because the exercise documents recovery procedures

Correct answer: C

Explanation: Deliberately injecting failures to verify automatic recovery is chaos testing, which applies the reliability pillar's principle of testing recovery procedures and automatically recovering from failure. Why the others are wrong - A: Access controls are a security concern, but this exercise tests failure recovery, not who can access what.; B: Saving money is incidental; the purpose of terminating servers is to prove the workload survives failures.; D: Documenting procedures is operational excellence, but the core goal here is validating automatic recovery - a reliability concern.

Q5. A company has finished migrating all of its applications to AWS. Its cloud team now continuously tunes performance, optimizes costs, and improves its operational processes month to month. Which phase of the AWS migration strategy is the company in?

A) Assess

B) Mobilize

C) Operate and optimize

D) Migrate and modernize

Correct answer: C

Explanation: Operate and optimize is the final phase of the AWS migration strategy: after workloads are running in AWS, the focus shifts to operating them well - tuning performance, optimizing cost, and continually improving processes. Why the others are wrong - A: The assess phase comes first: evaluating readiness, discovering the current state, and building the business case - long before workloads move.; B: The mobilize phase builds the foundation for migration - the landing zone, skills, and detailed migration plan - before large-scale migration begins.; D: Migrate and modernize is the phase in which applications are actually moved and modernized in waves. This company has already finished moving.

Q6. A hospital must retain MRI and X-ray images for seven years by law, but doctors rarely access images older than a year. Buying storage hardware for all of it up front is expensive. Which cloud economics concept BEST addresses this?

A) Move the archives to pay-per-gigabyte cloud storage instead of buying storage hardware up front

B) Economies of scale will make the MRI machines themselves cheaper

C) Deploy the archive in every AWS Region for global reach

D) High availability means the archived images can never be deleted

Correct answer: A

Explanation: Storing rarely accessed archives with per-gigabyte pricing converts a large up-front hardware purchase into a variable operating cost that scales with the actual data volume. Why the others are wrong - B: Economies of scale lower cloud service prices; they do not change the price of the hospital's medical equipment.; C: Global reach is about placing applications near users, not about archive storage costs.; D: High availability concerns uptime, not retention rules or deletion policies.

Q7. A logistics company must leave its data center in six months but also wants to modernize its databases over the next two years. Which migration approach fits?

A) Refactor every application before migrating anything

B) Rehost now to exit the data center quickly, then replatform in phases afterward

C) Repurchase a completely new warehouse system immediately

D) Refactor only the databases first, then migrate everything else together

Correct answer: B

Explanation: A staged strategy rehosts first to exit the data center quickly, then replatforms (for example, moving databases to managed services) once the workloads are stable on AWS. Why the others are wrong - A: Refactoring everything first would miss the six-month deadline.; C: Repurchasing replaces the system rather than migrating it, and takes longer than six months.; D: Refactoring the databases first consumes the timeline and misses the six-month data-center exit deadline; rehosting now exits on time while modernization proceeds in phases afterward.

Q8. A company runs EC2 instances in a VPC. Who is responsible for configuring security group rules that control inbound and outbound traffic to those instances?

A) AWS, because security groups are an AWS-managed firewall service

B) The customer, who defines the rules that control traffic to its instances

C) The internet service provider, as part of the network connection

D) AWS Config, which monitors and enforces the security group rule changes

Correct answer: B

Explanation: AWS provides the security group feature, but the customer writes the rules: which ports are open, which sources are allowed, and which instances the groups attach to. Why the others are wrong - A: Security groups are a customer-configured feature; AWS only provides the mechanism.; C: The ISP delivers connectivity but has no role in the customer's AWS firewall rules.; D: AWS Config records configuration changes and checks compliance, but it does not define security group rules.

Q9. A company already has a corporate identity system with usernames and passwords. How can employees access AWS without creating separate IAM users for each of them?

A) Use identity federation so employees sign in with their existing corporate identity provider

B) Share a single IAM user among all employees

C) Synchronize each employee's corporate password into a matching IAM user

D) Create an IAM user for each employee in bulk using the AWS CLI

Correct answer: A

Explanation: Identity federation lets users sign in with their existing corporate identity provider (via standards like SAML), so no separate IAM users or passwords are needed. Why the others are wrong - B: Sharing one user destroys accountability and cannot be revoked per person.; C: Password synchronization still creates and maintains separate IAM users; federation avoids that entirely.; D: Bulk creation still produces one IAM user per employee - exactly what the company wants to avoid.

Q10. A company wants to find IAM policies that grant access to people outside the organization and identify permissions that are no longer used. Which service helps with this?

A) Amazon GuardDuty

B) AWS WAF

C) IAM Access Analyzer

D) AWS Shield

Correct answer: C

Explanation: IAM Access Analyzer reviews policies and reports findings such as unused access and resource policies that grant access to external principals, helping teams remove excessive permissions. Why the others are wrong - A: GuardDuty detects threats such as compromised instances and malicious activity, not policy hygiene.; B: WAF filters malicious web traffic; it does not analyze IAM policies.; D: Shield protects against DDoS attacks; it has no visibility into IAM policies.

Q11. A company policy requires its encryption keys to be replaced with new key material every year automatically. Which service supports automatic annual key rotation?

A) AWS KMS

B) AWS Secrets Manager

C) AWS CloudHSM

D) AWS Certificate Manager

Correct answer: A

Explanation: AWS KMS supports automatic annual rotation of customer-managed keys, so the cryptographic material changes regularly without application changes. Why the others are wrong - B: Secrets Manager automates rotation of secrets such as database passwords and API keys - not encryption key material; automatic annual rotation of cryptographic keys is a KMS feature.; C: CloudHSM provides dedicated hardware security modules where the customer controls key management directly; managed automatic rotation of keys is a KMS capability.; D: ACM automatically renews TLS certificates for HTTPS; it has no role in rotating encryption key material - that is KMS.

Q12. A company tags resources with "Environment: Production" and "DataClassification: Confidential". What is the security governance benefit?

A) Automation and IAM policies can identify resources tagged Confidential and consistently require protections such as encryption

B) Tagging automatically encrypts any resource it is applied to

C) Tags replace the need for IAM policies

D) Tags are useful only for billing reports

Correct answer: A

Explanation: Consistent tagging lets governance automation find sensitive resources and apply the right controls uniformly. Why the others are wrong - B: Tags are labels; they do not encrypt anything by themselves.; C: Tags inform policies but do not replace identity and access control.; D: Billing allocation is one use of tags, but governance and automation are equally important.

Q13. A company wants developers to fully manage EC2 in the development account but have no access to production. What is the security best practice?

A) Give every developer administrator access in all accounts

B) Use the root user for production administration

C) Keep all workloads in one account and use environment tags (dev/prod) to separate them

D) Use separate AWS accounts with IAM permissions scoped to each environment

Correct answer: D

Explanation: Account separation plus scoped IAM policies ensure developers can work freely in development while production stays protected. Why the others are wrong - A: Broad admin access in production violates

least privilege and increases blast radius.; B: Root should never be used for daily administration.; C: Tags organize resources but do not enforce access boundaries; only separate accounts with scoped IAM policies truly isolate development from production.

Q14. A company must store Social Security numbers in a managed database, but its policy requires that even the database operator cannot read the plaintext values. Which encryption approach satisfies this?

A) Use SSE-S3, because the database operator manages those keys

B) Use TLS only, because it encrypts stored data

C) Use client-side encryption: encrypt the sensitive fields in the application with keys it manages before storing them

D) Use AWS CloudHSM, because client-side encryption is impossible without dedicated hardware

Correct answer: C

Explanation: Client-side encryption means the application encrypts data before sending it anywhere, keeping control of the keys (for example via KMS) - so even the database operator cannot read the plaintext fields. Why the others are wrong - A: With SSE-S3 or server-side database encryption, the service holds the keys and can decrypt the data.; B: TLS protects data in transit; it does not protect data once stored in the database.; D: Client-side encryption can use keys from AWS KMS; dedicated CloudHSM hardware is not required.

Q15. A company policy requires that all objects uploaded to S3 use server-side encryption. How can this be ENFORCED automatically across all accounts?

A) Apply an SCP that denies S3 uploads without server-side encryption across the organization

B) Configure a security group rule requiring encryption

C) Create a WAF rule that inspects S3 uploads

D) Create an AWS Config rule that flags unencrypted uploads and sends a weekly summary email

Correct answer: A

Explanation: Service Control Policies can deny s3:PutObject requests that do not include server-side encryption, enforcing the encryption standard preventively across every account in the organization. Why the others are wrong - B: Security groups control network traffic to instances; they cannot enforce S3 encryption settings.; C: WAF protects web applications from HTTP exploits; it does not govern S3 encryption.; D: A Config rule only detects and reports unencrypted uploads after they happen; it cannot prevent them. Enforcement requires the preventive SCP that denies the PutObject request itself.

Q16. A company lets team leads create IAM roles for their teams but must prevent them from granting more permissions than intended. Which feature sets the maximum permissions those roles can receive?

A) An SCP that denies iam:CreateRole outside an approved organizational unit

B) An IAM permissions boundary on the roles team leads can create

C) AWS IAM Access Analyzer, which alerts on unused permissions

D) Attaching the AWS managed ReadOnlyAccess policy to the team leads

Correct answer: B

Explanation: A permissions boundary is a managed policy that sets the maximum permissions an identity can receive, so delegated administrators can create roles without granting more access than the boundary allows - preventing privilege escalation. Why the others are wrong - A: An SCP can restrict where roles are created,

but it does not set a permissions ceiling on the roles themselves. The permissions boundary defines the maximum permissions.; C: Access Analyzer reports findings about access, including unused permissions, but it does not enforce a maximum permissions limit on roles.; D: ReadOnlyAccess would limit the team leads themselves. The question asks how to cap the permissions of the roles the leads create - that is what a permissions boundary does.

Q17. A hospital must keep patient data processing inside its own building for regulatory reasons but wants to use the same AWS APIs and tools it uses in the cloud. Which option fits?

A) AWS Storage Gateway with cached volumes in the hospital's data center

B) A VPN connection between two VPCs

C) AWS Outposts, which brings AWS infrastructure and services into the customer's own data center

D) An edge location upgraded to run databases

Correct answer: C

Explanation: AWS Outposts is a fully managed service that installs AWS-designed infrastructure in the customer's own facility, extending the same AWS APIs, tools, and services on premises for consistent hybrid operations. Why the others are wrong - A: Storage Gateway extends storage to on premises, but Outposts brings full AWS infrastructure, APIs, and services into the hospital's building.; B: A VPN connects networks; it does not provide AWS services on premises.; D: Edge locations cache content and do not host customer database workloads on premises.

Q18. A company must migrate a legacy application that cannot be containerized or modified and requires a full Windows Server environment running continuously. Which compute service is the BEST fit?

A) AWS Lambda

B) Amazon EC2

C) AWS Fargate

D) Amazon App Runner

Correct answer: B

Explanation: A legacy application that cannot be modified and needs a full operating system with persistent local state is a classic fit for EC2, where you manage the whole server. Why the others are wrong - A: Lambda requires code in supported runtimes and cannot run an unmodified legacy Windows application.; C: Fargate requires the workload to be containerized, which this application cannot be.; D: App Runner deploys containerized web applications and APIs, not unmodified legacy Windows servers.

Q19. A company stores application logs that are accessed once or twice a month, must be retrieved in milliseconds, and must survive the loss of a data center. Which S3 storage class is the BEST fit?

A) S3 Standard

B) S3 Glacier Instant Retrieval

C) S3 Standard-IA

D) S3 One Zone-IA

Correct answer: C

Explanation: S3 Standard-IA is designed for infrequently accessed data that still needs millisecond retrieval and resilience across multiple Availability Zones. Why the others are wrong - A: S3 Standard works but costs more than needed for data accessed only once or twice a month.; B: Glacier Instant Retrieval is for archive data, not for operational logs that are part of a working application.; D: One Zone-IA stores data in a single

Availability Zone, so it cannot survive a data center loss.

Q20. A company needs a relational database compatible with MySQL that was purpose-built by AWS for the cloud, with storage that grows automatically and continuous backup to Amazon S3. Which service fits BEST?

A) Amazon RDS for SQL Server

B) Amazon Aurora

C) Amazon Neptune

D) Amazon ElastiCache

Correct answer: B

Explanation: Amazon Aurora is AWS's cloud-native relational database, compatible with MySQL and PostgreSQL, with storage that auto-scales up to 128 TB and continuous backup to S3. Why the others are wrong - A: RDS for SQL Server is a managed version of Microsoft's engine, not an AWS purpose-built database.; C: Neptune is a graph database for relationship-heavy data, not a MySQL-compatible relational database.; D: ElastiCache is an in-memory caching service, not a relational database.

Q21. A company wants an isolated section of the AWS Cloud where it controls its own IP address range, subnets, and routing. Which AWS service or feature provides this?

A) Amazon VPC - a logically isolated virtual network that you define and control

B) An Availability Zone - a physically separate data center

C) An edge location - a site that caches content for CloudFront

D) A security group - a virtual firewall for EC2 instances

Correct answer: A

Explanation: Amazon VPC lets you provision a logically isolated section of the AWS Cloud where you define IP address ranges, subnets, route tables, and gateways. Why the others are wrong - B: An Availability Zone is a data center location you deploy into, not a network you define.; C: Edge locations cache content; they are not isolated networks you control.; D: Security groups control traffic to instances; they do not define the network itself.

Q22. A company wants to analyze thousands of customer reviews to determine sentiment (positive, negative, neutral) and extract key phrases. Which AWS service should it use?

A) Amazon Comprehend

B) Amazon Polly

C) Amazon Rekognition

D) Amazon Translate

Correct answer: A

Explanation: Amazon Comprehend uses NLP to find insights in text, including sentiment analysis, entity detection, and key-phrase extraction. Why the others are wrong - B: Polly converts text to speech; it does not analyze meaning.; C: Rekognition analyzes images and video, not text sentiment.; D: Translate converts text between languages; it does not determine sentiment.

Q23. A developer's team wants to define AWS infrastructure using a familiar programming language such as Python or TypeScript instead of writing JSON or YAML templates directly. Which AWS tool meets this need?

A) AWS Cloud Development Kit (AWS CDK)

B) Boto3, the AWS SDK for Python, since it lets developers use Python to create AWS resources

C) AWS Elastic Beanstalk, since developers deploy applications by uploading code
D) AWS CloudFormation Designer, since it provides a visual way to build templates
Correct answer: A
Explanation: The AWS Cloud Development Kit lets developers define cloud infrastructure as code using familiar programming languages, and it synthesizes those definitions into CloudFormation templates for deployment. Why the others are wrong - B: Boto3 makes imperative API calls from scripts; it does not define declarative, versioned infrastructure templates the way the CDK does.; C: Elastic Beanstalk deploys applications onto a managed platform; it does not let developers define infrastructure as code in a programming language.; D: Designer is a drag-and-drop visual tool; the requirement is to write infrastructure definitions in a familiar programming language.

Q24. A company is migrating a fleet of physical servers to AWS. For each server, it wants to know which applications and dependencies must move together. Which approach, using AWS migration tools, gives this information?
A) Exporting the CMDB spreadsheets the team maintains and matching server names manually
B) Running network port scans between servers to infer which ones communicate
C) Migrating one server at a time and rolling back whenever something breaks
D) Running AWS Application Discovery Service to inventory servers and map their dependencies
Correct answer: D
Explanation: AWS Application Discovery Service collects inventory and dependency information about on-premises servers, so migration waves can be planned with the correct applications grouped together. Why the others are wrong - A: Manual spreadsheets go stale and miss undocumented dependencies; Application Discovery Service collects this inventory automatically.; B: Port scans show network traffic, not application-level dependencies; the Discovery Service maps which applications depend on which servers.; C: Trial-and-error migration risks repeated outages; discovering dependencies first lets the team plan waves that move dependent servers together.

Q25. A team deploys containerized microservices and wants to keep using Kubernetes APIs, but it does not want to manage any cluster servers or worker nodes itself. Which combination meets this requirement?
A) Amazon EC2 with Kubernetes installed manually
B) AWS Lambda functions
C) AWS Fargate with Amazon ECS
D) Amazon EKS with AWS Fargate
Correct answer: D
Explanation: Amazon EKS provides managed Kubernetes control planes, and AWS Fargate runs the containers serverlessly, so the team uses standard Kubernetes APIs with no servers or nodes to manage. Why the others are wrong - A: Self-installed Kubernetes on EC2 leaves the team managing every server and the control plane - the opposite of the requirement.; B: Lambda runs functions, not Kubernetes workloads; it does not provide the Kubernetes API.; C: Fargate with ECS is serverless containers but uses the ECS API, not Kubernetes.

Q26. A company streams website click events continuously, needs to flag suspicious patterns within seconds, and wants a live dashboard of site activity. Which combination BEST fits?
A) A nightly batch job writing to Amazon RDS

B) Amazon SQS with a single EC2 consumer
C) Amazon Kinesis for ingestion, AWS Lambda for real-time detection, and Amazon QuickSight for the live dashboard
D) Amazon Athena querying last month's logs
Correct answer: C
Explanation: Kinesis ingests the continuous event stream, Lambda processes each event within seconds for fraud detection, and QuickSight visualizes the live activity - a real-time pipeline with no servers to manage. Why the others are wrong - A: A nightly batch job detects fraud a day late and cannot power a live dashboard.; B: A single EC2 consumer is a bottleneck and a single point of failure for a continuous high-volume stream.; D: Athena over last month's logs is retrospective analysis, not real-time detection or live dashboards.

Q27. A startup's web application has unpredictable traffic: almost nothing at night, then huge spikes when it is mentioned on social media. The founders refuse any upfront hardware purchase. Which AWS pricing approach fits this workload, and why?
A) Buy Reserved Instances sized for the peak traffic, all year round
B) Purchase and host their own servers sized for peak load
C) Lease Dedicated Hosts on a three-year term
D) On-Demand pay-as-you-go: run capacity when traffic arrives and pay only for what is used, with no upfront commitment
Correct answer: D
Explanation: Pay-as-you-go matches cost to actual use: capacity grows with the spikes and shrinks at night, the bill follows real usage, and nothing is bought in advance - the natural fit for unpredictable demand. Why the others are wrong - A: Reserving for peak means paying for idle capacity through every quiet hour; commitments fit steady usage, not spikes.; B: Owned servers sized for peak sit idle most of the time and require exactly the upfront purchase the founders rejected.; C: Dedicated Hosts add a long-term commitment for single-tenancy the startup never asked for.

Q28. A startup wants billing alerts delivered to the finance team's email whenever spend is forecasted to exceed budget. Which services work together to deliver this?
A) AWS Cost Explorer sending alerts through Amazon SES
B) AWS CloudTrail writing to Amazon CloudWatch Logs
C) AWS Budgets publishing notifications through Amazon SNS
D) AWS Config publishing findings through Amazon EventBridge
Correct answer: C
Explanation: AWS Budgets evaluates actual and forecasted spend against thresholds and publishes alert notifications to SNS topics, which deliver them to subscribed email addresses. Why the others are wrong - A: Cost Explorer performs cost analysis but has no alerting capability, and SES is a bulk email service rather than the notification path.; B: CloudTrail and CloudWatch Logs handle API auditing and operational monitoring, not budget threshold notifications.; D: Config evaluates resource compliance; it is not the service that watches budget thresholds.

Q29. A team sets an AWS Budget for $10,000 and wants an alert when the forecast shows they will exceed it - even if actual spending is still below. Which budget capability supports this?
A) A forecasted budget alert in AWS Budgets

B) A cost allocation tag budget
C) A Savings Plan utilization budget
D) An AWS Cost Explorer alert
Correct answer: A
Explanation: AWS Budgets can alert on forecasted spend, not just actual spend - so the team is warned when projections show the $10,000 budget will be exceeded. Why the others are wrong - B: There is no such thing as a tag budget; tags organize costs, budgets monitor them.; C: Savings Plan budgets track commitment utilization, a pricing-model metric, not a dollar forecast.; D: Cost Explorer does not send alerts at all; alerting is Budgets' role.

Q30. A company on Enterprise support wants AWS experts to formally assess its workloads against best practices and produce improvement recommendations. Which Enterprise benefit is this?
A) Infrastructure Event Management
B) AWS IQ project staffing
C) A Well-Architected Framework review
D) Trusted Advisor's basic checks
Correct answer: C
Explanation: Enterprise support includes Well-Architected reviews, where AWS (often via the TAM) evaluates workloads against the Framework's pillars and recommends improvements. Why the others are wrong - A: Infrastructure Event Management supports planned events like launches; it is not an architecture assessment.; B: AWS IQ is a separate expert marketplace, not an Enterprise support benefit.; D: Basic Trusted Advisor checks are automated best-practice flags available to all plans, not a formal expert review.