CompTIA Cloud+ (CV0-004) — One-Page Study Guide

BareMetalCyber.com | Cybersecurity Audio Academy
baremetalcyber.com/cybersecurity-audio-academy

A) Exam Snapshot

- Exam: CompTIA Cloud+ (V4) - CV0-004
- Max questions: 90 (maximum)
- Time limit: 90 minutes
- Question types: Multiple choice + performance-based questions (PBQs)
- Passing score: 750 (scale 100-900)
- Delivery: Pearson VUE (testing center or online)

B) Domain Weights

Domain	Weight
Cloud Architecture	23%
Deployment	19%
Operations	17%
Security	19%
DevOps Fundamentals	10%
Troubleshooting	12%

C) Core Workflow

- Clarify the scenario and requirements (availability, security, performance, cost, constraints).
- Map the target cloud architecture (service and deployment models, network and identity boundaries).
- Plan deployment or migration steps (resources, dependencies, sequencing, rollback).
- Harden and configure (identity and access, network controls, encryption, secrets, policy).
- Operate with observability (logs, metrics, alerts) and lifecycle management (scaling, patching, backup).
- Automate repeatable work (IaC templates, CI/CD pipeline steps, configuration baselines).
- Troubleshoot using evidence (baselines, recent changes, logs, metrics) and verify the fix.
- Report outcomes (documentation, diagrams, tickets, compliance artifacts) and adjust governance.

D) High-Yield Concepts

- Cloud service models: IaaS vs PaaS vs SaaS (who manages what).
- Deployment models: public, private, hybrid, multicloud; tenancy and isolation basics.
- Shared responsibility: provider vs customer duties for security and operations.
- Networking: VPC/VNet concepts, subnets, routing, security groups vs NACLs, load balancing.
- Identity and access: least privilege, RBAC, federation, MFA, service accounts, key rotation.
- Compute: VMs vs containers; scaling patterns (horizontal vs vertical) and autoscaling triggers.
- Storage: object vs block vs file; snapshots, replication, and performance tradeoffs.
- Observability: metrics vs logs vs traces; alert thresholds, SLO/SLI basics [VERIFY: objective emphasis].
- Backup and DR: RPO vs RTO; backup types; restore testing and retention.
- Security controls: encryption in transit/at rest, KMS/key custody, secrets management, WAF, vuln mgmt.
- Automation and DevOps: version control, CI/CD gates, IaC drift, immutable vs mutable infrastructure.
- Troubleshooting patterns: isolate layer, compare to baseline, correlate to change window, validate end-to-end.

E) Common Traps

- Confusing service model vs deployment model (IaaS/PaaS/SaaS is not public/private).
- Assuming the cloud provider handles customer-side security (IAM, data classification, config).
- Choosing the wrong storage type for the workload (IOPS/latency vs durability vs cost).
- Treating stateful and stateless network controls as interchangeable (security groups vs NACLs).
- Ignoring time and order: DNS propagation, eventual consistency, dependency sequencing, change windows.
- Jumping into troubleshooting without checking recent changes, baselines, and monitoring evidence.
- Fixing symptoms without validating the full path (client -> network -> compute -> storage -> identity).
- Overlooking governance basics: tagging, resource ownership, cost controls, and documentation artifacts.

F) Cheat Sheet

- Key artifacts to recognize: architecture diagram, network map, IAM policy, security group/NACL ruleset.
- Operational evidence: monitoring dashboard, alert history, logs, change ticket, incident timeline.
- Automation evidence: IaC template (e.g., Terraform/CloudFormation-style), pipeline definition, repo history.
- Resilience evidence: backup policy, snapshot schedule, restore test record, RPO/RTO statement.
- Security evidence: vulnerability scan report, patch status, key management settings, audit log sample.
- Cost and governance evidence: tags, cost report, budget alert, resource lifecycle/retirement record.

G) Exam-Day Tactics

- First pass: answer fast wins; flag long scenarios; keep momentum.
- PBQs: skip initially if allowed; return with a time box and a clear plan.
- Read for qualifiers: best, first, most likely, least; match the verb to the task.
- Eliminate by constraints: security, availability, performance, cost, compliance, supportability.
- When stuck, pick the option that adds measurable evidence (logs, monitoring, validation) before changes.
- Use the last 10-15 minutes for flagged items and PBQ cleanup; answer every question.

H) 30-Minute Final Review Plan

- 5 min: skim domain weights and identify the weakest 1-2 areas.
- 10 min: review high-yield distinctions (models, IAM, network controls, storage types, RPO/RTO).
- 5 min: rehearse a generic troubleshooting flow using baselines and change correlation.
- 5 min: review common traps and force a 'what evidence proves it' mindset.
- 5 min: reset pacing plan (PBQs last, flag-and-return, answer all).

Source: official exam objectives & exam details. Quick review only; practice required.