EDUSUM

#1 Online Certification Guide

CV0-002

Cloud+

A Success Guide to Prepare-
CompTIA Cloud+

edusum.com

Table of Contents

Introduction to CV0-002 Exam on CompTIA Cloud+

Use this quick start guide to collect all the information about CompTIA Cloud+ (CV0-002) Certification exam. This study guide provides a list of objectives and resources that will help you prepare for items on the CV0-002 CompTIA Cloud+ exam. The Sample Questions will help you identify the type and difficulty level of the questions and the Practice Exams will make you familiar with the format and environment of an exam. You should refer this guide carefully before attempting your actual CompTIA Cloud Plus certification exam.

The CompTIA Cloud+ certification is mainly targeted to those candidates who want to build their career in Cloud Computing domain. The CompTIA Cloud+ exam verifies that the candidate possesses the fundamental knowledge and proven skills in the area of CompTIA Cloud Plus.

CompTIA CV0-002 Certification Details:

Exam Name	CompTIA Cloud+
Exam Code	CV0-002
Exam Price	$302 (USD)
Duration	90 min
Number of Questions	90
Passing Score	750 / 900
Schedule Exam	Pearson VUE
Sample Questions	CompTIA Cloud+ Sample Questions
Practice Exam	**CompTIA CV0-002 Certification Practice Exam**

CompTIA CV0-002 Exam Syllabus:

Topic	Details
Configuration and Deployment 24%	
Given a scenario, analyze system requirements to ensure successful system deployment.	1. Appropriate commands, structure, tools, and automation/orchestration as needed 2. Platforms and applications 3. Interaction of cloud components and services 1. Network components 2. Application components 3. Storage components 4. Compute components 5. Security components 4. Interaction of non-cloud components and services 5. Baselines 6. Target hosts 7. Existing systems 8. Cloud architecture 9. Cloud elements/target objects
Given a scenario, execute a provided deployment plan.	1. Apply the change management process 1. Approvals 2. Scheduling 2. Refer to documentation and follow standard operating procedures 3. Execute workflow 4. Configure automation and orchestration, where appropriate, for the system being deployed 5. Use commands and tools as needed 6. Document results
Given a scenario, analyze system requirements to determine if a given testing plan is appropriate.	1. Underlying environmental considerations included in the testing plan 1. Shared components 2. Production vs. development vs. QA 3. Sizing 4. Performance 5. High availability 6. Connectivity 7. Data integrity 8. Proper function 9. Replication 10. Load balancing 11. Automation/orchestration

Topic	Details
	2. Testing techniques 1. Vulnerability testing 2. Penetration testing 3. Load testing
Given a scenario, analyze testing results to determine if the testing was successful in relation to given system requirements.	1. Consider success factor indicators of the testing environment 1. Sizing 2. Performance 3. Availability 4. Connectivity 5. Data integrity 6. Proper functionality 2. Document results 3. Baseline comparisons 4. SLA comparisons 5. Cloud performance fluctuation variables
Given a scenario, analyze sizing, subnetting, and basic routing for a provided deployment of the virtual network.	1. Cloud deployment models Public Private Hybrid Community 2. Network components 3. Applicable port and protocol considerations when extending to the cloud 4. Determine configuration for the applicable platform as it applies to the network 1. VPN 2. IDS/IPS 3. DMZ 4. VXLAN 5. Address space required 6. Network segmentation and microsegmentation 5. Determine if cloud resources are consistent with the SLA and/or change management requirements
Given a scenario, analyze CPU and memory sizing for a provided deployment.	1. Available vs. proposed resources 1. CPU 2. RAM 2. Memory technologies

Topic	Details
	1. Bursting and ballooning 2. Overcommitment ratio 3. CPU technologies 1. Hyperthreading 2. VT-x 3. Overcommitment ratio 4. Effect to HA/DR 5. Performance considerations 6. Cost considerations 7. Energy savings Dedicated compute environment vs. shared compute environment
Given a scenario, analyze the appropriate storage type and protection capability for a provided deployment.	1. Requested IOPS and read/ write throughput 2. Protection capabilities 1. High availability Failover zones 2. Storage replication Regional Multiregional Synchronous and asynchronous 3. Storage mirroring 4. Cloning 5. Redundancy level/factor 3. Storage types 1. NAS 2. DAS 3. SAN 4. Object storage 4. Access protocols 5. Management differences 6. Provisioning model 1. Thick provisioned 2. Thin provisioned 3. Encryption requirements

Topic	Details
	4. Tokenization 7. Storage technologies 1. Deduplication technologies 2. Compression technologies 8. Storage tiers 9. Overcommitting storage 10. Security configurations for applicable platforms 1. ACLs 2. Obfuscation 3. Zoning 4. User/host authentication and authorization
Given a scenario, analyze characteristics of the workload (storage, network, compute) to ensure a successful migration.	1. Migration types 1. P2V 2. V2V 3. V2P 4. P2P 5. Storage migrations 6. Online vs. offline migrations 2. Source and destination format of the workload 1. Virtualization format 2. Application and data portability 3. Network connections and data transfer methodologies 4. Standard operating procedures for the workload migration 5. Environmental constraints 1. Bandwidth 2. Working hour restrictions 3. Downtime impact 4. Peak timeframes 5. Legal restrictions 6. Follow-the-sun constraints/time zones
Given a scenario, apply elements required to extend the infrastructure into a given cloud solution.	1. Identity management elements 1. Identification 2. Authentication

Topic	Details
	3. Authorization Approvals Access policy 4. Federation Single sign-on 2. Appropriate protocols given requirements 3. Element considerations to deploy infrastructure services such as: 1. DNS 2. DHCP 3. Certificate services 4. Local agents 5. Antivirus 6. Load balancer 7. Multifactor authentication 8. Firewall 9. IPS/IDS
Security 16%	
Given a scenario, apply security configurations and compliance controls to meet given cloud infrastructure requirements.	1. Company security policies 2. Apply security standards for the selected platform 3. Compliance and audit requirements governing the environment 1. Laws and regulations as they apply to the data 4. Encryption technologies 1. IPSec 2. SSL/TLS 3. Other ciphers 5. Key and certificate management 1. PKI 6. Tunneling protocols 1. L2TP 2. PPTP 3. GRE 7. Implement automation and orchestration processes as applicable

Topic	Details
	8. Appropriate configuration for the applicable platform as it applies to compute 1. Disabling unneeded ports and services 2. Account management policies 3. Host-based/software firewalls 4. Antivirus/anti-malware software 5. Patching 6. Deactivating default accounts
Given a scenario, apply the appropriate ACL to the target objects to meet access requirements according to a security template.	1. Authorization to objects in the cloud 1. Processes 2. Resources Users Groups System Compute Networks Storage 3. Services 2. Effect of cloud service models on security implementations 3. Effect of cloud deployment models on security implementations 4. Access control methods 1. Role-based administration 2. Mandatory access controls 3. Discretionary access contros 4. Non-discretionary access contros 5. Multifactor authentication 6. Single sign-on
Given a cloud service model, implement defined security technologies to meet given security requirements.	1. Data classification 2. Concepts of segmentation and microsegmentation 1. Network 2. Storage 3. Compute

Topic	Details
	3. Use encryption as defined 4. Use multifactor authentication as defined 5. Apply defined audit/ compliance requirements
Given a cloud service model, apply the appropriate security automation technique to the target system.	1. Tools 1. APIs 2. Vendor applications 3. CLI 4. Web GUI 5. Cloud portal 2. Techniques 1. Orchestration 2. Scripting 3. Custom programming 3. Security services 1. Firewall 2. Antivirus/anti-malware 3. IPS/IDS 4. HIPS 4. Impact of security tools to systems and services 1. Scope of impact 5. Impact of security automation techniques as they relate to the criticality of systems 1. Scope of impact
Maintenance 18%	
Given a cloud service model, determine the appropriate methodology to apply given patches.	1. Scope of cloud elements to be patched 1. Hypervisors 2. Virtual machines 3. Virtual appliances 4. Networking components 5. Applications 6. Storage components 7. Clusters 2. Patching methodologies and standard operating procedures

Topic	Details
	1. Production vs. development vs. QA 2. Rolling update 3. Blue-green deployment 4. Failover cluster 3. Use order of operations as it pertains to elements that will be patched 4. Dependency considerations
Given a scenario, apply the appropriate automation tools to update cloud elements.	1. Types of updates 1. Hotfix 2. Patch 3. Version update 4. Rollback 2. Automation workflow 1. Runbook management Single node 2. Orchestration Multiple nodes Multiple runbooks 3. Activities to be performed by automation tools 1. Snapshot 2. Cloning 3. Patching 4. Restarting 5. Shut down 6. Maintenance mode 7. Enable/disable alerts
Given a scenario, apply an appropriate backup or restore method.	1. Backup types 1. Snapshot/redirect-on-write 2. Clone 3. Full 4. Differential 5. Incremental 6. Change block/delta tracking 2. Backup target 1. Replicas 2. Local

Topic	Details
	3. Remote 3. Other considerations 1. SLAs 2. Backup schedule 3. Configurations 4. Objects 5. Dependencies 6. Online/offline
Given a cloud-based scenario, apply appropriate disaster recovery methods.	1. DR capabilities of a cloud service provider 2. Other considerations 1. SLAs for DR 2. RPO 3. RTO 4. Corporate guidelines 5. Cloud service provider guidelines 6. Bandwidth or ISP limitations 7. Techniques 8. Site mirroring 9. Replication 10. File transfer 11. Archiving 12. Third-party sites
Given a cloud-based scenario, apply the appropriate steps to ensure business continuity.	1. Business continuity plan 1. Alternate sites 2. Continuity of operations 3. Connectivity 4. Edge sites 5. Equipment 6. Availability 7. Partners/third parties 2. SLAs for BCP and HA
Given a scenario, apply the appropriate maintenance automation technique to the target objects.	1. Maintenance schedules 2. Impact and scope of maintenance tasks 3. Impact and scope of maintenance automation techniques 4. Include orchestration as appropriate 5. Maintenance automation tasks 1. Clearing logs 2. Archiving logs 3. Compressing drives

Topic	Details
	4. Removing inactive accounts 5. Removing stale DNS entries 6. Removing orphaned resources 7. Removing outdated rules from firewall 8. Removing outdated rules from security 9. Resource reclamation 10. Maintain ACLs for the target object
Management 20%	
Given a scenario, analyze defined metrics to determine the presence of an abnormality and/or forecast future needed cloud resources.	1. Monitoring 1. Target object baselines 2. Target object anomalies 3. Common alert methods/messaging 4. Alerting based on deviation from baseline 5. Event collection 2. Event correlation 3. Forecasting resource capacity 1. Upsize/increase 2. Downsize/decrease 4. Policies in support of event collection Policies to communicate alerts appropriately
Given a scenario, determine the appropriate allocation of cloud resources.	1. Resources needed based on cloud deployment models 1. Hybrid 2. Community 3. Public 4. Private 2. Capacity/elasticity of cloud environment 3. Support agreements 1. Cloud service model maintenance responsibility 4. Configuration management tool 5. Resource balancing techniques 6. Change management 1. Advisory board 2. Approval process 3. Document actions taken

Topic	Details
	CMDB Spreadsheet
Given a scenario, determine when to provision/deprovision cloud resources.	1. Usage patterns 2. Cloud bursting 1. Auto-scaling technology 3. Cloud provider migrations 4. Extending cloud scope 5. Application life cycle 1. Application deployment 2. Application upgrade 3. Application retirement 4. Application replacement 5. Application migration 6. Application feature use Increase/decrease 6. Business need change 1. Mergers/acquisitions/divestitures 2. Cloud service requirement changes 3. Impact of regulation and law changes
Given a scenario, implement account provisioning techniques in a cloud environment to meet security and policy requirements.	1. Identification 2. Authentication methods 1. Federation Single sign-on 3. Authorization methods 1. ACLs 2. Permissions 4. Account life cycle 5. Account management policy 1. Lockout 2. Password complexity rules 6. Automation and orchestration activities 1. User account creation 2. Permission settings

Topic	Details
	3. Resource access 4. User account removal 5. User account disablement
Given a scenario, analyze deployment results to confirm they meet the baseline.	1. Procedures to confirm results 1. CPU usage 2. RAM usage 3. Storage utilization 4. Patch versions 5. Network utilization 6. Application version 7. Auditing enable 8. Management tool compliance
Given a specific environment and related data (e.g., performance, capacity, trends), apply appropriate changes to meet expected criteria.	1. Analyze performance trends 2. Refer to baselines 3. Refer to SLAs 4. Tuning of cloud target objects 1. Compute 2. Network 3. Storage 4. Service/application resources 5. Recommend changes to meet expected performance/capacity 1. Scale up/down (vertically) 2. Scale in/out (horizontally)
Given SLA requirements, determine the appropriate metrics to report.	1. Chargeback/showback models 1. Reporting based on company policies 2. Reporting based on SLAs 2. Dashboard and reporting 1. Elasticity usage 2. Connectivity 3. Latency 4. Capacity 5. Overall utilization 6. Cost 7. Incidents 8. Health

Topic	Details
	9. System availability Uptime Downtime
Troubleshooting 22%	
Given a scenario, troubleshoot a deployment issue.	1. Common issues in the deployments 1. Breakdowns in the workflow 2. Integration issues related to different cloud platforms 3. Resource contention 4. Connectivity issues 5. Cloud service provider outage 6. Licensing issues 7. Template misconfiguration 8. Time synchronization issues 9. Language support 10. Automation issues
Given a scenario, troubleshoot common capacity issues.	1. Exceeded cloud capacity boundaries 1. Compute 2. Storage 3. Networking IP address limitations Bandwidth limitations 4. Licensing 5. Variance in number of users 6. API request limit 7. Batch job scheduling issues 2. Deviation from original baseline 3. Unplanned expansions
Given a scenario, troubleshoot automation/orchestration issues.	1. Breakdowns in the workflow 1. Account mismatch issues 2. Change management failure 3. Server name changes 4. IP address changes 5. Location changes 6. Version/feature mismatch 7. Automation tool incompatibility 8. Job validation issue
Given a scenario, troubleshoot connectivity issues.	1. Common networking issues 1. Incorrect subnet

Topic	Details
	2. Incorrect IP address 3. Incorrect gateway 4. Incorrect routing 5. DNS errors 6. QoS issues 7. Misconfigured VLAN or VXLAN 8. Misconfigured firewall rule 9. Insufficient bandwidth 10. Latency 11. Misconfigured MTU/MSS 12. Misconfigured proxy 2. Network tool outputs 3. Network connectivity tools 1. ping 2. tracert/traceroute 3. telnet 4. netstat 5. nslookup/dig 6. ipconfig/ifconfig 7. route 8. arp 9. ssh 10. tcpdump 4. Remote access tools for troubleshooting
Given a scenario, troubleshoot security issues.	1. Authentication issues 1. Account lockout/expiration 2. Authorization issues 3. Federation and single sign-on issues 4. Certificate expiration 5. Certification misconfiguration 6. External attacks 7. Internal attacks 8. Privilege escalation 9. Internal role change 10. External role change 11. Security device failure 12. Incorrect hardening settings 13. Unencrypted communication 14. Unauthorized physical access 15. Unencrypted data 16. Weak or obsolete security technologies 17. Insufficient security controls and processes 18. Tunneling or encryption issues

Topic	Details
Given a scenario, explain the troubleshooting methodology.	Always consider corporate policies, procedures and impacts before implementing changes 1. Identify the problem 1. Question the user and identify user changes to computer and perform backups before making changes 2. Establish a theory of probable cause (question the obvious) 1. If necessary, conduct internal or external research based on symptoms 3. Test the theory to determine cause 1. Once theory is confirmed, determine the next steps to resolve the problem 2. If the theory is not confirmed, re-establish a new theory or escalate 4. Establish a plan of action to resolve the problem and implement the solution 5. Verify full system functionality and, if applicable, implement preventive measures 6. Document findings, actions and outcomes

CV0-002 Sample Questions:

01. What cloud model delivers server hardware with no operating system?
a) IaaS
b) PaaS
c) SaaS
d) CaaS

02. A constantly changing six-digit numerical token is used in what type of cloud service?
a) XML
b) TLS
c) SSL
d) MFA
e) JSON

03. SaaS orchestration systems are whose responsibility in the public cloud?
a) Customer
b) Provider
c) Automation vendor
d) DevOps

04. What application tracks a process from start to finish?
a) API
b) NTP
c) Workflow
d) Orchestration

05. Hank goes to his local bank and inserts his card into the ATM and then enters his PIN on the keypad. What type of authentication is he participating in?
a) SSO
b) Two-factor
c) LDAP
d) User based

06. MFA tokens can be obtained where?
(Choose two.)
a) Python app
b) Smartphone app
c) Automation systems
d) Keyfob
e) Cloud vendor management dashboard

07. Scott is planning his company's upload of stored data to the cloud. What are two common storage migration types?
(Choose two.)
a) Physical to virtual
b) Block to object
c) Online
d) Offline
e) Synchronous
f) Asynchronous

08. Object tracking should be aligned with which of the following?
a) SLA
b) VPC
c) RDP
d) JSON

09. Larken is reviewing the SLA and statement of responsibility with their community cloud provider PaaS. Who does the responsibility for stored data integrity in the cloud belong to?
a) Cloud provider
b) Compliance agency
c) Cloud customer
d) Shared responsibility

10. Which cloud characteristic allows you to pay for only the services used?
a) Bursting
b) Metering
c) Chargeback
d) Pay-as-you-grow

Answers to CV0-002 Exam Questions:

Question: 01 Answer: a	Question: 02 Answer: d	Question: 03 Answer: b	Question: 04 Answer: c	Question: 05 Answer: b
Question: 06 Answer: b, d	Question: 07 Answer: c, d	Question: 08 Answer: a	Question: 09 Answer: c	Question: 10 Answer: d

Note: If you find any typo or data entry error in these sample questions, we request you to update us by commenting on this page or write an email on feedback@edusum.com