EDUSUM

#1 Online Certification Guide

COMPTIA CV0-002

CompTIA Cloud Plus Certification Questions & Answers

Exam Summary – Syllabus –Questions

CV0-002

CompTIA Cloud+

90 Questions Exam – 750/900 Cut Score – Duration of 90 minutes

Table of Contents:

Know Your CV0-002 Certification Well:

The CV0-002 is best suitable for candidates who want to gain knowledge in the CompTIA Infrastructure. Before you start your CV0-002 preparation you may struggle to get all the crucial Cloud Plus materials like CV0-002 syllabus, sample questions, study guide.

But don't worry the CV0-002 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the CV0-002 syllabus?
- How many questions are there in the CV0-002 exam?
- Which Practice test would help me to pass the CV0-002 exam at the first attempt?

Passing the CV0-002 exam makes you CompTIA Cloud+. Having the Cloud Plus certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

CompTIA CV0-002 Cloud Plus Certification Details:

Exam Name	CompTIA Cloud+
Exam Code	CV0-002
Exam Price	$338 (USD)
Duration	90 mins
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**

CV0-002 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 • Network components • Application components • Storage components • Compute components • 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 • Approvals • 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 • Shared components Storage Compute Network • Production vs. development vs. QA

Topic	Details
	• Sizing • Performance • High availability • Connectivity • Data integrity • Proper function • Replication • Load balancing • Automation/orchestration 2. Testing techniques • Vulnerability testing • Penetration testing • 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 • Sizing • Performance • Availability • Connectivity • Data integrity • 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

Topic	Details
	• VPN • IDS/IPS • DMZ • VXLAN • Address space required • 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 • CPU • RAM 2. Memory technologies • Bursting and ballooning • Overcommitment ratio 3. CPU technologies • Hyperthreading • VT-x • Overcommitment ratio 4. Effect to HA/DR 5. Performance considerations 6. Cost considerations 7. Energy savings 8. 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 • High availability Failover zones • Storage replication Regional Multiregional Synchronous and asynchronous • Storage mirroring

Topic	Details
	• Cloning • Redundancy level/factor 3. Storage types • NAS • DAS • SAN • Object storage 4. Access protocols 5. Management differences 6. Provisioning model • Thick provisioned • Thin provisioned • Encryption requirements • Tokenization 7. Storage technologies • Deduplication technologies • Compression technologies 8. Storage tiers 9. Overcommitting storage 10. Security configurations for applicable platforms • ACLs • Obfuscation • Zoning • User/host authentication and authorization
Given a scenario, analyze characteristics of the workload (storage, network, compute) to ensure a successful migration.	1. Migration types • P2V • V2V • V2P • P2P • Storage migrations • Online vs. offline migrations 2. Source and destination format of the workload • Virtualization format

Topic	Details
	• Application and data portability 3. Network connections and data transfer methodologies 4. Standard operating procedures for the workload migration 5. Environmental constraints • Bandwidth • Working hour restrictions • Downtime impact • Peak timeframes • Legal restrictions • 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 • Identification • Authentication • Authorization Approvals Access policy • Federation Single sign-on 2. Appropriate protocols given requirements 3. Element considerations to deploy infrastructure services such as: • DNS • DHCP • Certificate services • Local agents • Antivirus • Load balancer • Multifactor authentication • Firewall • IPS/IDS

Topic	Details
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 • Laws and regulations as they apply to the data 4. Encryption technologies • IPSec • SSL/TLS • Other ciphers 5. Key and certificate management • PKI 6. Tunneling protocols • L2TP • PPTP • GRE 7. Implement automation and orchestration processes as applicable 8. Appropriate configuration for the applicable platform as it applies to compute • Disabling unneeded ports and services • Account management policies • Host-based/software firewalls • Antivirus/anti-malware software • Patching • 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 • Processes • Resources Users

Topic	Details
	Groups System ○ Compute ○ Networks ○ Storage • Services 2. Effect of cloud service models on security implementations 3. Effect of cloud deployment models on security implementations 4. Access control methods • Role-based administration • Mandatory access controls • Discretionary access controls • Non-discretionary access controls • Multifactor authentication • 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 • Network • Storage • Compute 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 • APIs • Vendor applications • CLI • Web GUI • Cloud portal 2. Techniques

Topic	Details
	• Orchestration • Scripting • Custom programming 3. Security services • Firewall • Antivirus/anti-malware • IPS/IDS • HIPS 4. Impact of security tools to systems and services • Scope of impact 5. Impact of security automation techniques as they relate to the criticality of systems • 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 • Hypervisors • Virtual machines • Virtual appliances • Networking components • Applications • Storage components • Clusters 2. Patching methodologies and standard operating procedures • Production vs. development vs. QA • Rolling update • Blue-green deployment • Failover cluster 3. Use order of operations as it pertains to elements that will be patched 4. Dependency considerations

Topic	Details
Given a scenario, apply the appropriate automation tools to update cloud elements.	1. Types of updates • Hotfix • Patch • Version update • Rollback 2. Automation workflow • Runbook management Single node • Orchestration Multiple nodes Multiple runbooks 3. Activities to be performed by automation tools • Snapshot • Cloning • Patching • Restarting • Shut down • Maintenance mode • Enable/disable alerts
Given a scenario, apply an appropriate backup or restore method.	1. Backup types • Snapshot/redirect-on-write • Clone • Full • Differential • Incremental • Change block/delta tracking 2. Backup target • Replicas • Local • Remote 3. Other considerations • SLAs • Backup schedule

Topic	Details
	• Configurations • Objects • Dependencies • Online/offline
Given a cloud-based scenario, apply appropriate disaster recovery methods.	1. DR capabilities of a cloud service provider 2. Other considerations • SLAs for DR • RPO • RTO • Corporate guidelines • Cloud service provider guidelines • Bandwidth or ISP limitations • Techniques • Site mirroring • Replication • File transfer • Archiving • Third-party sites
Given a cloud-based scenario, apply the appropriate steps to ensure business continuity.	1. Business continuity plan • Alternate sites • Continuity of operations • Connectivity • Edge sites • Equipment • Availability • 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 • Clearing logs • Archiving logs

Topic	Details
	• Compressing drives • Removing inactive accounts • Removing stale DNS entries • Removing orphaned resources • Removing outdated rules from firewall • Removing outdated rules from security • Resource reclamation • 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 • Target object baselines • Target object anomalies • Common alert methods/messaging • Alerting based on deviation from baseline • Event collection 2. Event correlation 3. Forecasting resource capacity • Upsize/increase • 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 • Hybrid • Community • Public • Private 2. Capacity/elasticity of cloud environment 3. Support agreements • Cloud service model maintenance responsibility

Topic	Details
	4. Configuration management tool 5. Resource balancing techniques 6. Change management • Advisory board • Approval process • Document actions taken CMDB Spreadsheet
Given a scenario, determine when to provision/deprovision cloud resources.	1. Usage patterns 2. Cloud bursting • Auto-scaling technology 3. Cloud provider migrations 4. Extending cloud scope 5. Application life cycle • Application deployment • Application upgrade • Application retirement • Application replacement • Application migration • Application feature use Increase/decrease 6. Business need change • Mergers/acquisitions/divestitures • Cloud service requirement changes • 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 • Federation Single sign-on 3. Authorization methods • ACLs • Permissions

Topic	Details
	4. Account life cycle 5. Account management policy • Lockout • Password complexity rules 6. Automation and orchestration activities • User account creation • Permission settings • Resource access • User account removal • User account disablement
Given a scenario, analyze deployment results to confirm they meet the baseline.	1. Procedures to confirm results • CPU usage • RAM usage • Storage utilization • Patch versions • Network utilization • Application version • Auditing enable • 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 • Compute • Network • Storage • Service/application resources 5. Recommend changes to meet expected performance/capacity • Scale up/down (vertically) • Scale in/out (horizontally)
Given SLA requirements, determine the appropriate metrics to report.	1. Chargeback/showback models • Reporting based on company policies

Topic	Details
	• Reporting based on SLAs 2. Dashboard and reporting • Elasticity usage • Connectivity • Latency • Capacity • Overall utilization • Cost • Incidents • Health • System availability Uptime Downtime
Troubleshooting - 22%	
Given a scenario, troubleshoot a deployment issue.	1. Common issues in the deployments • Breakdowns in the workflow • Integration issues related to different cloud platforms • Resource contention • Connectivity issues • Cloud service provider outage • Licensing issues • Template misconfiguration • Time synchronization issues • Language support • Automation issues
Given a scenario, troubleshoot common capacity issues.	1. Exceeded cloud capacity boundaries • Compute • Storage • Networking IP address limitations Bandwidth limitations • Licensing

Topic	Details
	• Variance in number of users • API request limit • Batch job scheduling issues 2. Deviation from original baseline 3. Unplanned expansions
Given a scenario, troubleshoot automation/orchestration issues.	1. Breakdowns in the workflow • Account mismatch issues • Change management failure • Server name changes • IP address changes • Location changes • Version/feature mismatch • Automation tool incompatibility • Job validation issue
Given a scenario, troubleshoot connectivity issues.	1. Common networking issues • Incorrect subnet • Incorrect IP address • Incorrect gateway • Incorrect routing • DNS errors • QoS issues • Misconfigured VLAN or VXLAN • Misconfigured firewall rule • Insufficient bandwidth • Latency • Misconfigured MTU/MSS • Misconfigured proxy 2. Network tool outputs 3. Network connectivity tools • ping • tracert/traceroute • telnet • netstat • nslookup/dig • ipconfig/ifconfig

Topic	Details
	• route • arp • ssh • tcpdump 4. Remote access tools for troubleshooting
Given a scenario, troubleshoot security issues.	1. Authentication issues • 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
Given a scenario, explain the troubleshooting methodology.	Always consider corporate policies, procedures and impacts before implementing changes 1. Identify the problem • 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) • If necessary, conduct internal or external research based on symptoms 3. Test the theory to determine cause • Once theory is confirmed, determine the next steps to resolve the problem

Topic	Details
	• If the theory is not confirmed, reestablish 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

CompTIA CV0-002 Sample Questions:

Question: 1

Your organization tracks private cloud usage by department for billing purposes. What type of model is this?

a) Service level agreement
b) Agile
c) Waterfall
d) Chargeback

Answer: d

Question: 2

Regulations dictate that specific types of documents be stored permanently. Metadata must be added to each stored item to facilitate retrieval. Which term best describes this storage system?

a) Content addressed storage
b) Cloud backup
c) Storage area network
d) Storage tiers

Answer: a

Question: 3

Compared to Type II hypervisors, Type I hypervisors generally have lower:

a) numbers of VMs per host
b) requirements for host overhead
c) numbers of hosts installed in datacenters
d) costs

Answer: b

Question: 4

In a RAID 6 environment a technician is trying to calculate how many read operations would be made. How many read operations would be required in RAID 6?

a) One
b) Four
c) Two
d) Three

Answer: d

Question: 5

What is the maximum amount of RAM supported by Citrix XenServer 6.1?

a) 64GB
b) 96GB
c) 128GB
d) 192GB

Answer: c

Question: 6

Why are shadow page tables necessary?

a) VMs don’t always support dynamic memory.
b) VMs cannot access host memory directly.
c) RAM depletion means writing pages to disk.
d) They trigger page faults.

Answer: b

Question: 7

For which of the following protocols will an administrator configure a trap to collect system state data?

a) SNMP
b) FTPS
c) IPMI
d) SMTP

Answer: a

Question: 8

A busy on-premises file server needs to be migrated to the cloud as a virtual machine. Which migration strategy should you employ?

a) Online P2V
b) Online V2P
c) Offline P2V
d) Offline V2P

Answer: c

Question: 9

Which of the following hypervisor types requires the least overhead?

a) Type II
b) open source
c) Type I
d) hosted

Answer: c

Question: 10

You need a central location to view log data gathered from 50 Linux servers. What should you configure?

a) Syslog forwarding
b) WMI forwarding
c) IPMI forwarding
d) SNMP forwarding

Answer: a

Study Guide to Crack CompTIA Cloud Plus CV0-002 Exam:

- Getting details of the CV0-002 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the CV0-002 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the CompTIA provided training for CV0-002 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the CV0-002 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on CV0-002 practice tests is must. Continuous practice will make you an expert in all syllabus areas.