EDUSUM

#1 Online Certification Guide

COMPTIA CV0-003

CompTIA Cloud+ Certification Questions & Answers

Exam Summary – Syllabus –Questions

CV0-003

CompTIA Cloud+

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

Table of Contents:

Know Your CV0-003 Certification Well:

The CV0-003 is best suitable for candidates who want to gain knowledge in the CompTIA Infrastructure. Before you start your CV0-003 preparation you may struggle to get all the crucial Cloud+ materials like CV0-003 syllabus, sample questions, study guide.

But don't worry the CV0-003 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 CV0-003 syllabus?
- How many questions are there in the CV0-003 exam?
- Which Practice test would help me to pass the CV0-003 exam at the first attempt?

Passing the CV0-003 exam makes you CompTIA Cloud+. Having the Cloud+ 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 CV0-003 Cloud+ Certification Details:

Exam Name	CompTIA Cloud+
Exam Code	CV0-003
Exam Price	$338 (USD)
Duration	90 mins
Number of Questions	90
Passing Score	750 / 900
Schedule Exam	**CompTIA Marketplace** **Pearson VUE**
Sample Questions	**CompTIA Cloud+ Sample Questions**
Practice Exam	**CompTIA CV0-003 Certification Practice Exam**

CV0-003 Syllabus:

Topic	Details
Cloud Architecture and Design - 13%	
Compare and contrast the different types of cloud models.	- Deployment models • Public • Private • Hybrid • Community • Cloud within a cloud • Multicloud • Multitenancy - Service models • Infrastructure as a Service (IaaS) • Platform as a Service (PaaS) • Software as a Service (SaaS) - Advanced cloud services • Internet of Things (IoT) • Serverless • Machine learning/Artificial intelligence (AI) - Shared responsibility model
Explain the factors that contribute to capacity planning.	- Requirements • Hardware • Software • Budgetary • Business need analysis - Standard templates • Per-user • Socket-based • Volume-based • Core-based • Subscription

Topic	Details
	- Licensing - User density - System load - Trend analysis • Baselines • Patterns • Anomalies - Performance capacity planning
Explain the importance of high availability and scaling in cloud environments.	- Hypervisors • Affinity • Anti-affinity - Oversubscription • Compute • Network • Storage - Regions and zones - Applications - Containers - Clusters - High availability of network functions • Switches • Routers • Load balancers • Firewalls - Avoid single points of failure - Scalability • Auto-scaling • Horizontal scaling • Vertical scaling • Cloud bursting
Given a scenario, analyze the solution design in support of the business requirements.	- Requirement analysis • Software • Hardware

Topic	Details
	• Integration • Budgetary • Compliance • Service-level agreement (SLA) • User and business needs • Security • Network requirements 1. Sizing 2. Subnetting 3. Routing - Environments • Development • Quality assurance (QA) • Staging • Blue-green • Production • Disaster recovery (DR) - Testing techniques • Vulnerability testing • Penetration testing • Performance testing • Regression testing • Functional testing • Usability testing
Security - 20%	
Given a scenario, configure identity and access management.	- Identification and authorization • Privileged access management • Logical access management • Account life-cycle management 1. Provision and deprovision accounts • Access controls 1. Role-based 2. Discretionary 3. Non-discretionary 4. Mandatory

Topic	Details
	- Directory services • Lightweight directory access protocol (LDAP) - Federation - Certificate management - Multifactor authentication (MFA) - Single sign-on (SSO) • Security assertion markup language (SAML) - Public key infrastructure (PKI) - Secret management - Key management
Given a scenario, secure a network in a cloud environment.	- Network segmentation • Virtual LAN (VLAN)/Virtual extensible LAN (VXLAN)/Generic network virtualization encapsulation (GENEVE) • Micro-segmentation • Tiering - Protocols • Domain name service (DNS) 1. DNS over HTTPS (DoH)/DNS over TLS (DoT) 2. DNS security (DNSSEC) • Network time protocol (NTP) 1. Network time security (NTS) • Encryption 1. IPSec 2. Transport layer security (TLS) 3. Hypertext transfer protocol secure (HTTPS) • Tunneling 1. Secure Shell (SSH) 2. Layer 2 tunneling protocol (L2TP)/Point-to-point tunneling protocol (PPTP) 3. Generic routing encapsulation (GRE) - Network services • Firewalls 1. Stateful 2. Stateless • Web application firewall (WAF) • Application delivery controller (ADC)

Topic	Details
	• Intrusion protection system (IPS)/Intrusion detection system (IDS) • Data loss prevention (DLP) • Network access control (NAC) • Packet brokers - Log and event monitoring - Network flows - Hardening and configuration changes • Disabling unnecessary ports and services • Disabling weak protocols and ciphers • Firmware upgrades • Control ingress and egress traffic 1. Allow list (previously known as whitelisting) or blocklist (previously known as blacklisting) 2. Proxy servers • Distributed denial of service (DDoS) protection
Given a scenario, apply the appropriate OS and application security controls.	- Policies • Password complexity • Account lockout • Application approved list (previously known as whitelisting) • Software feature • User/group - User permissions - Antivirus/anti-malware/endpoint detection and response (EDR) - Host-based IDS (HIDS)/Host-based IPS (HIPS) - Hardened baselines • Single function - File integrity - Log and event monitoring - Configuration management - Builds • Stable • Long-term support (LTS) • Beta • Canary

Topic	Details
	- Operating system (OS) upgrades - Encryption • Application programming interface (API) endpoint • Application • OS • Storage • Filesystem - Mandatory access control - Software firewall
Given a scenario, apply data security and compliance controls in cloud environments.	- Encryption - Integrity • Hashing algorithms • Digital signatures • File integrity monitoring (FIM) - Classification - Segmentation - Access control - Impact of laws and regulations • Legal hold - Records management • Versioning • Retention • Destruction • Write once read many - Data loss prevention (DLP) - Cloud access security broker (CASB)
Given a scenario, implement measures to meet security requirements.	- Tools • Vulnerability scanners • Port scanners - Vulnerability assessment • Default and common credential scans • Credentialed scans • Network-based scans

Topic	Details
	• Agent-based scans • Service availabilities - Security patches • Hot fixes • Scheduled updates • Virtual patches • Signature updates • Rollups - Risk register - Prioritization of patch application - Deactivate default accounts - Impacts of security tools on systems and services - Effects of cloud service models on security implementation
Explain the importance of incident response procedures.	- Preparation • Documentation • Call trees • Training • Tabletops • Documented incident types/categories • Roles and responsibilities - Incident response procedures • Identification 1. Scope • Investigation • Containment, eradication, and recovery 1. Isolation 2. Evidence acquisition 3. Chain of custody 4. Root cause analysis • Post-incident and lessons learned
Deployment - 23%	
Given a scenario, integrate components into a cloud solution.	- Subscription services • File subscriptions

Topic	Details
	• Communications 1. Email 2. Voice over IP (VoIP) 3. Messaging • Collaboration • Virtual desktop infrastructure (VDI) • Directory and identity services • Cloud resources 1. IaaS 2. PaaS 3. SaaS - Provisioning resources • Compute • Storage • Network - Application • Serverless - Deploying virtual machines (VMs) and custom images - Templates • OS templates • Solution templates - Identity management - Containers • Configure variables • Configure secrets • Persistent storage - Auto-scaling - Post-deployment validation
Given a scenario, provision storage in cloud environments.	- Types • Block 1. Storage area network (SAN) - Zoning • File 1. Network attached storage (NAS)

Topic	Details
	• Object 1. Tenants 2. Buckets - Tiers • Flash • Hybrid • Spinning disks • Long-term - Input/output operations per second (IOPS) and read/write - Protocols • Network file system (NFS) • Common Internet file system (CIFS) • Internet small computer system interface (iSCSI) • Fibre Channel (FC) • Non-volatile memory express over fabrics (NVMe-oF) - Redundant array of inexpensive disks (RAID) • 0 • 1 • 5 • 6 • 10 - Storage system features • Compression • Deduplication • Thin provisioning • Thick provisioning • Replication - User quotas - Hyperconverged - Software-defined storage (SDS)
Given a scenario, deploy cloud networking solutions.	- Services • Dynamic host configuration protocol (DHCP)

Topic	Details
	• NTP • DNS • Content delivery network (CDN) • IP address management (IPAM) - Virtual private networks (VPNs) • Site-to-site • Point-to-point • Point-to-site • IPSec • Multiprotocol label switching (MPLS) - Virtual routing • Dynamic and static routing • Virtual network interface controller (vNIC) • Subnetting - Network appliances • Load balancers • Firewalls - Virtual private cloud (VPC) • Hub and spoke • Peering - VLAN/VXLAN/GENEVE - Single root input/output virtualization (SR-IOV) - Software-defined network (SDN)
Given a scenario, configure the appropriate compute sizing for a deployment.	- Virtualization • Hypervisors 1. Type 1 2. Type 2 • Simultaneous multi-threading (SMT) • Dynamic allocations • Oversubscription - Central processing unit (CPU)/virtual CPU (vCPU) - Graphics processing unit (GPU)

Topic	Details
	• Virtual 1. Shared • Pass-through - Clock speed/Instructions per cycle (IPC) - Hyperconverged - Memory • Dynamic allocation • Ballooning
Given a scenario, perform cloud migrations.	- Physical to virtual (P2V) - Virtual to virtual (V2V) - Cloud-to-cloud migrations • Vendor lock-in • PaaS or SaaS migrations 1. Access control lists (ACLs) 2. Firewalls - Storage migrations • Block • File • Object - Database migrations • Cross-service migrations • Relational • Non-relational
Operations and Support - 22%	
Given a scenario, configure logging, monitoring, and alerting to maintain operational status.	- Logging • Collectors 1. Simple network management protocol (SNMP) 2. Syslog • Analysis • Severity categorization • Audits • Types 1. Access/authentication

Topic	Details
	2. System 3. Application • Automation • Trending - Monitoring • Baselines • Thresholds • Tagging • Log scrubbing • Performance monitoring 1. Application 2. Infrastructure components • Resource utilization • Availability 1. SLA-defined uptime requirements • Verification of continuous monitoring activities • Service management tool integration - Alerting • Common messaging methods • Enable/disable alerts 1. Maintenance mode • Appropriate responses • Policies for categorizing and communicating alerts
Given a scenario, maintain efficient operation of a cloud environment.	- Confirm completion of backups - Life-cycle management • Roadmaps • Old/current/new versions • Upgrading and migrating systems • Deprecations or end of life - Change management - Asset management • Configuration management database (CMDB) - Patching • Features or enhancements

Topic	Details
	• Fixes for broken or critical infrastructure or applications • Scope of cloud elements to be patched 1. Hypervisors 2. VMs 3. Virtual appliances 4. Networking components 5. Applications 6. Storage components 7. Firmware 8. Software 9. OS • Policies 1. n-1 • Rollbacks - Impacts of process improvements on systems - Upgrade methods • Rolling upgrades • Blue-green • Canary • Active-passive • Development/QA/production/DR - Dashboard and reporting • Tagging • Costs 1. Chargebacks 2. Showbacks • Elasticity usage • Connectivity • Latency • Capacity • Incidents • Health • Overall utilization • Availability
Given a scenario, optimize cloud environments.	- Right-sizing • Auto-scaling • Horizontal scaling

Topic	Details
	• Vertical scaling • Cloud bursting - Compute • CPUs • GPUs • Memory • Containers - Storage • Tiers 1. Adaptive optimization • IOPS • Capacity • Deduplication • Compression - Network • Bandwidth • Network interface controllers (NICs) • Latency • SDN • Edge computing 1. CDN - Placement • Geographical • Cluster placement • Redundancy • Colocation - Device drivers and firmware • Generic • Vendor • Open source
Given a scenario, apply proper automation and orchestration techniques.	- Infrastructure as code • Infrastructure components and their integration

Topic	Details
	- Continuous integration/continuous deployment (CI/CD) - Version control - Configuration management • Playbook - Containers - Automation activities • Routine operations • Updates • Scaling • Shutdowns • Restarts • Create internal APIs - Secure scripting • No hardcoded passwords • Use of individual service accounts • Password vaults • Key-based authentication - Orchestration sequencing
Given a scenario, perform appropriate backup and restore operations.	- Backup types • Incremental • Differential • Full • Synthetic full • Snapshot - Backup objects • Application-level backup • Filesystem backup • Database dumps • Configuration files - Backup targets • Tape • Disk

Topic	Details
	• Object - Backup and restore policies • Retention • Schedules • Location • SLAs • Recovery time objective (RTO) • Recovery point objective (RPO) • Mean time to recovery (MTTR) • 3-2-1 rule 1. Three copies of data 2. Two different media 3. One copy off site - Restoration methods • In place • Alternate location • Restore files • Snapshot
Given a scenario, perform disaster recovery tasks.	- Failovers - Failback - Restore backups - Replication - Network configurations - On-premises and cloud sites • Hot • Warm • Cold - Requirements • RPO • RTO • SLA • Corporate guidelines - Documentation • DR kit

Topic	Details
	• Playbook • Network diagram - Geographical datacenter requirements
Troubleshooting - 22%	
Given a scenario, use the troubleshooting methodology to resolve cloud-related issues.	- Always consider corporate policies, procedures, and impacts before implementing changes. 1. Identify the problem - Question the user and identify user changes to the computer and perform backups before making changes - Inquire regarding environmental or infrastructure changes 2. Establish a theory of probable cause (question the obvious) - If necessary, conduct external or internal research based on symptoms 3. Test the theory to determine cause - Once the theory is confirmed, determine the next steps to resolve the problem - 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 the findings, actions, and outcomes throughout the process.
Given a scenario, troubleshoot security issues.	- Privilege • Missing • Incomplete • Escalation • Keys - Authentication - Authorization - Security groups • Network security groups • Directory security groups

Topic	Details
	- Keys and certificates • Expired • Revoked • Trust • Compromised • Misconfigured - Misconfigured or misapplied policies - Data security issues • Unencrypted data • Data breaches • Misclassification • Lack of encryption in protocols • Insecure ciphers - Exposed endpoints - Misconfigured or failed security appliances • IPS • IDS • NAC • WAF - Unsupported protocols - External/internal attacks
Given a scenario, troubleshoot deployment issues.	- Connectivity issues • Cloud service provider (CSP) or Internet service provider (ISP) outages - Performance degradation • Latency - Configurations • Scripts - Applications in containers - Misconfigured templates - Missing or incorrect tags - Insufficient capacity

Topic	Details
	• Scaling configurations • Compute • Storage • Bandwidth issues • Oversubscription - Licensing issues - Vendor-related issues • Migrations of vendors or platforms • Integration of vendors or platforms • API request limits • Cost or billing issues
Given a scenario, troubleshoot connectivity issues.	- Network security group misconfigurations • ACL • Inheritance - Common networking configuration issues • Peering • Incorrect subnet • Incorrect IP address • Incorrect IP space • Routes 1. Default 2. Static 3. Dynamic • Firewall 1. Incorrectly administered micro-segmentation • Network address translation (NAT) 1. VPN 2. Source 3. Destination • Load balancers 1. Methods 2. Headers 3. Protocols 4. Encryption 5. Back ends 6. Front ends • DNS records

Topic	Details
	• VLAN/VXLAN/GENEVE • Proxy • Maximum transmission unit (MTU) • Quality of service (QoS) • Time synchronization issues - Network troubleshooting tools • ping • tracert/traceroute • flushdns • ipconfig/ifconfig/ip • nslookup/dig • netstat/ss • route • arp • curl • Packet capture • Packet analyzer • OpenSSL client
Given a scenario, troubleshoot common performance issues.	- Resource utilization • CPU • GPU • Memory • Storage 1. I/O 2. Capacity • Network bandwidth • Network latency • Replication • Scaling - Application • Memory management • Service overload - Incorrectly configured or failed load balancing

Topic	Details
Given a scenario, troubleshoot automation or orchestration issues.	- Account mismatches - Change management failures - Server name changes - IP address changes - Location changes - Version/feature mismatch - Automation tool incompatibility • Deprecated features • API version incompatibility - Job validation issue - Patching failure

CompTIA CV0-003 Sample Questions:

Question: 1

Which of the following high availability solutions would a cloud service provider use when deploying Software as a Service?

a) Virtual switches
b) Multipathing
c) Load balancing
d) Clustering servers

Answer: d

Question: 2

Which of the following storage provisioning methods is implemented at the hardware level of a SAN and can be completed in either a soft or hard basis?

a) LUN masking
b) Network share creation
c) Zoning
d) Multipathing

Answer: c

Question: 3

Which of the following is the meaning of IaaS?

a) IT as a Service
b) Information as a Service
c) Infrastructure as a Service
d) Identity as a Service

Answer: c

Question: 4

Which of the following should an administrator use when marking VLAN traffic?

a) Virtual Local Area Network tagging
b) Network Address Translation
c) Subnetting
d) Port Address Translation

Answer: a

Question: 5

Which of the following commands provides measurements of round-trip network latency?

a) ping
b) route
c) arp
d) nslookup

Answer: a

Question: 6

Which of the following methods can an Administrator use to force an array to allow data to be distributed one node at a time in a private cloud implementation?

a) Least connections
b) Least used
c) Best bandwidth
d) Round robin

Answer: d

Question: 7

Which of the following allows authentication based on something you are?
(Select TWO)

a) Passwords
b) Access badge
c) Retina scan
d) Key fobs
e) Voice recognition
f) PIN

Answer: c, e

Question: 8

A community name is used by:

a) WMI
b) SMTP
c) SNMP
d) SMS

Answer: c

Question: 9

Which of the following will allow an administrator to quickly revert a VM back to a previous state?

a) Metadata
b) Snapshots
c) Extended metadata
d) Cloning

Answer: b

Question: 10

Which of the following is the meaning of SaaS?

a) Solutions as a Service
b) Software as a Service
c) Servers as a Service
d) Security as a Service

Answer: b

Study Guide to Crack CompTIA Cloud+ CV0-003 Exam:

- Getting details of the CV0-003 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 CV0-003 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 CV0-003 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 CV0-003 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 CV0-003 practice tests is must. Continuous practice will make you an expert in all syllabus areas.