COMPTIA CV0-003

CompTIA Cloud Plus Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

CV0-003

CompTIA Cloud+

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

EDUSUM
#1 Online Certification Guide

Table of Contents:

Discover More about the CV0-003 Certification 2

CompTIA CV0-003 Cloud Plus Certification Details: 2

CV0-003 Syllabus:...3

Cloud Architecture and Design - 13% 3

Security - 20% 6

Deployment - 23%...11

Operations and Support - 22% 15

Troubleshooting - 22%..21

Broaden Your Knowledge with CompTIA CV0-003 Sample Questions: 26

Avail the Study Guide to Pass CompTIA CV0-003 Cloud Plus Exam: 29

Career Benefits: 29

Discover More about the CV0-003 Certification

Are you interested in passing the CompTIA CV0-003 exam? First discover, who benefits from the CV0-003 certification. The CV0-003 is suitable for a candidate if he wants to learn about Infrastructure. Passing the CV0-003 exam earns you the CompTIA Cloud+ title.

While preparing for the CV0-003 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The CV0-003 PDF contains some of the most valuable preparation tips and the details and instant access to useful **CV0-003 study materials just at one click.**

CompTIA CV0-003 Cloud Plus Certification Details:

Exam Name	CompTIA Cloud+
Exam Code	CV0-003
Exam Price	$358 (USD)
Duration	90 mins
Number of Questions	90
Passing Score	750 / 900
Books / Training	**Virtual Lab** **Study Guides** **eLearning** **Instructor-Led Training**
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

Topic	Details
	- Volume-based - Core-based - Subscription - 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

Topic	Details
	• Horizontal scaling • Vertical scaling • Cloud bursting
Given a scenario, analyze the solution design in support of the business requirements.	- Requirement analysis • Software • Hardware • 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

Topic	Details
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 - 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

Topic	Details
	• 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) • 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

Topic	Details
	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 - Operating system (OS) upgrades - Encryption • Application programming interface (API) endpoint • Application • OS • Storage • Filesystem

Topic	Details
	- 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 • Agent-based scans • Service availabilities

Topic	Details
	- 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

Topic	Details
Deployment - 23%	
Given a scenario, integrate components into a cloud solution.	- Subscription services • File subscriptions • 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

Topic	Details
	- 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) • 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

Topic	Details
	- 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) • 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

Topic	Details
	- 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) • 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

Topic	Details
	- 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 2. System 3. Application • Automation • Trending - Monitoring • Baselines • Thresholds • Tagging • Log scrubbing • Performance monitoring 1. Application 2. Infrastructure components

Topic	Details
	• 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 • 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

Topic	Details
	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 • Vertical scaling • Cloud bursting - Compute

Topic	Details
	• 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	- Infrastructure as code • Infrastructure components and their integration

Topic	Details
orchestration techniques.	- 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

Topic	Details
	- Backup targets • Tape • Disk • 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

Topic	Details
	- Requirements • RPO • RTO • SLA • Corporate guidelines - Documentation • DR kit • 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

Topic	Details
	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 - 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

Topic	Details
	- 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 - 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

Topic	Details
	- 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 • 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

Topic	Details
	• 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
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

Topic	Details
	- Job validation issue - Patching failure

Broaden Your Knowledge with CompTIA CV0-003 Sample Questions:

Question: 1

Quotas are a mechanism for enforcing what?

a) Limits
b) Rules
c) Access restrictions
d) Virtualization

Answer: a

Question: 2

You have been tasked with migrating a VM to a new host computer. Which migration process would be required?

a) P2V
b) V2P
c) P2P
d) V2V

Answer: d

Question: 3

You are planning your migration to a virtual environment. Which of the following physical servers should be migrated first?
(Choose two.)

a) A development server
b) A server that is running a non–mission-critical application and is not heavily utilized day to day
c) A highly utilized database server
d) A server running a mission-critical application

Answer: a, b

Question: 4

Which of the following gives a cloud provider the ability to distribute resources on an as-needed basis to the cloud consumer and in turn helps to improve efficiency and reduce costs?

a) Elasticity
b) Shared resources
c) Infrastructure consolidation
d) Network isolation

Answer: b

Question: 5

Capacity management has responsibility for ensuring that the capacity of the IT service is optimally matched to what?

a) Demand
b) Future trends
c) Procedures
d) Availability

Answer: a

Question: 6

With PKI, which key is used to validate a digital signature?

a) Private key
b) Public key
c) Secret key
d) Signing key

Answer: b

Question: 7

After a successful P2V migration, which of the following tests, if any, should be completed on the new VM?

a) Testing is not required.
b) Remove all unnecessary software.
c) Verify the IP address, DNS, and other network configurations.
d) Run a monitoring program to verify compute resources.

Answer: c

Question: 8

An administrator is trying to enable hardware-assisted virtualization in the BIOS of a computer and notices it is not an option. He checks the specification on the manufacturer's website and finds that the system should support hardware-assisted virtualization. What is most likely the reason why he can't enable it?

a) The BIOS needs a firmware update.
b) The BIOS is corrupt.
c) Hardware-assisted virtualization is enabled in the operating system, not the BIOS.
d) The firmware is corrupt.

Answer: a

Question: 9

Which of the following are requirements for adequate application performance when using synchronous replication?

(Choose two.)

a) Object storage
b) Low latency
c) Multipathing
d) High-speed links

Answer: b, c

Question: 10

Sean configures a web application to allow content managers to upload files to the website. What type of access control model is Sean using?

a) DAC
b) MAC
c) RBAC
d) GBAC

Answer: c

Avail the Study Guide to Pass CompTIA CV0-003 Cloud Plus Exam:

- Find out about the CV0-003 syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **CV0-003 syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.
- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the CV0-003 training. Joining the CompTIA provided training for CV0-003 exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **CV0-003 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. CV0-003 practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

- Passing the CV0-003 exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.

Here Is the Trusted Practice Test for the CV0-003 Certification

EduSum.Com is here with all the necessary details regarding the CV0-003 exam. We provide authentic practice tests for the CV0-003 exam. What do you gain from these practice tests? You get to experience the real exam-like questions made by industry experts and get a scope to improve your performance in the actual exam. Rely on EduSum.Com for rigorous, unlimited two-month attempts on the **CV0-003 practice tests**, and gradually build your confidence. Rigorous practice made many aspirants successful and made their journey easy towards grabbing the CompTIA Cloud+.

Start Online Practice of CV0-003 Exam by visiting URL
https://www.edusum.com/comptia/cv0-003-comptia-cloud