CompTIA Cloud+ Certification Exam Objectives

EXAM NUMBER: CV0-001

CompTIA

About the Exam

Candidates are encouraged to use this document to prepare for the CompTIA Cloud+ certification. This certification will validate that the candidate has the knowledge and skills required to understand:

- **Standard cloud terminologies/methodologies**
- **How to implement, maintain and deliver cloud technologies and infrastructures (e.g., server, network, storage and virtualization technologies)**
- **Aspects of IT security and use of industry best practices related to cloud implementations and the application of virtualization**

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an entry-level IT professional.

CompTIA AUTHORIZED MATERIALS USE POLICY

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse or condone utilizing any content provided by unauthorized third-party training sites (aka "brain dumps"). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA's exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the **CompTIA Certification Exam Policies**. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the **CompTIA Candidate Agreement**. If a candidate has a question as to whether study materials are considered unauthorized (aka "brain dumps"), he/she should contact CompTIA at examsecurity@comptia.org to confirm.

PLEASE NOTE

The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes or tasks pertaining to each objective may also be included on the exam although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

TEST DETAILS

Required exam	CV0-001
Number of questions	100
Type of questions	Multiple choice
Length of test	90 minutes
Recommended experience	• At least 24–36 months of work experience in IT networking, network storage or datacenter administration • Familiarity with any major hypervisor technologies for server virtualization, though vendor-specific certifications in virtualization are not required • CompTIA Network+ and/or CompTIA Server+, though CompTIA certifications are not required
Passing score	750 (on a scale of 100–900)

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented:

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 Cloud Concepts and Models	12%
2.0 Virtualization	19%
3.0 Infrastructure	21%
4.0 Resource Management	13%
5.0 Security	16%
6.0 Systems Management	11%
7.0 Business Continuity in the Cloud	8%
Total	**100%**

1.0 Cloud Concepts and Models

1.1 Compare and contrast cloud services.

- SaaS (according to NIST)
- IaaS (according to NIST)
- PaaS (according to NIST)
- CaaS
- XaaS
- DaaS
- BPaaS
- Accountability and responsibility based on service models

1.2 Compare and contrast cloud delivery models and services.

- Private
- Public
- Hybrid
- Community
- On-premise vs. off-premise hosting
- Accountability and responsibility based on delivery models
- Security differences between models
  - Multi-tenancy issues
  - Data segregation
  - Network isolation
  - Check laws and regulations
- Functionality and performance validation based on chosen delivery model
- Orchestration platforms

1.3 Summarize cloud characteristics and terms.

- Elasticity
- On-demand self-service/just-in-time service
- Pay-as-you-grow
- Chargeback
- Ubiquitous access
- Metering resource pooling
- Multi-tenancy
- Cloud bursting
- Rapid deployment
- Automation

1.4 Explain object storage concepts.

- Object ID
- Metadata
- Data/blob
- Extended metadata
- Policies
- Replicas
- Access control

2.0 Virtualization

2.1 Explain the differences between hypervisor types.

- **Type I and Type II**
  - Bare metal vs. OS dependent
  - Performance and overhead considerations
  - Hypervisor-specific system requirements
- **Proprietary vs. open source**
- **Consumer vs. enterprise use**
  - Workstation vs. infrastructure

2.2 Install, configure and manage virtual machines and devices.

- **Creating, importing and exporting template and virtual machines**
- **Install guest tools**
  - Drives
  - Management tools
- **Snapshots and cloning**
- **Image backups vs. file backups**
- **Virtual NIC**
  - Virtual network
  - IP address
  - Default gateway
  - Netmask
  - Bridging
- **Virtual disks**
  - Limits
  - SCSI/ATA ID
- **Virtual switches**
  - VLAN
  - Interface configuration
- **VLAN**
  - Assign IDs
  - Bind interfaces
- **VSAN**
  - Assign IDs

2.3 Given a scenario, perform virtual resource migration.

- **Establish requirements**
- **Maintenance scheduling**
- **Reasons**
  - Performance issues
  - Testing
  - Upgrading
  - Utilization
- **Storage migration**
  - Virtual vs. physical
- **Online vs. offline migrations**
- **Physical to Virtual (P2V)**
- **Virtual to Virtual (V2V)**
- **Virtual to Physical (V2P)**

2.4 Explain the benefits of virtualization in a cloud environment.

- **Shared resources**
- **Elasticity**
  - Time to service/mean time to implement
  - Resource pooling
  - Scalable
  - Available
  - Portable
- **Network and application isolation**
- **Infrastructure consolidation**
- **Virtual datacenter creation**

2.5 Compare and contrast virtual components used to construct a cloud environment.

- **Virtual network components**
  - Virtual NIC
  - Virtual HBA
  - Virtual router
- **Shared memory**
- **Virtual CPU**
- **Storage virtualization**
  - Shared storage
  - Clustered storage
  - NPIV

3.0 Infrastructure

3.1 Compare and contrast various storage technologies.

- **Network Attached Storage (NAS)**
  - File level access
  - Shared storage
- **Direct Attached Storage (DAS)**
  - Block level access
  - Dedicated storage
- **Storage Area Network (SAN)**
  - Block level access
  - Shared storage
  - HBAs
  - LUN masking
  - Zoning
  - WWN
  - Fibre Channel protocols
- **Different access protocols**
  - FCoE
  - FC
  - Ethernet
  - iSCSI
- **Protocols and applications**
  - IP
  - FCP
  - iSCSI
- **Management differences**

3.2 Explain storage configuration concepts.

- **Disk types**
  - SSD vs. spinning
  - Interfaces types
  - Access speed
- **Tiering**
  - Performance levels of each tier
  - Policies
- **RAID levels**
  - RAID 1
  - RAID 0
  - RAID 1+0
  - RAID 0+1
  - RAID 5
  - RAID 6
- **File system types**
  - UFS
  - EXT
  - NTFS
  - FAT
  - VMFS
  - ZFS

3.3 Execute storage provisioning.

- **Creating LUNs**
- **Creating network shares**
- **Zoning and LUN masking**
- **Multipathing**
- **Implications of adding capacity to a NAS and SAN**
  - Impact to operations
  - Downtime
  - Best practices

3.4 Given a scenario, implement appropriate network configurations.

- **NAT**
- **PAT**
- **Subnetting/supernetting**
- **VLAN and VLAN tagging**
- **Network port configurations**
- **Switching and routing in physical and virtual environments**
  - Routing tables

3.5 Explain the importance of network optimization.

- WAN
- LAN
- MAN
- QoS
- Bandwidth
- Latency
- Compression
- Caching
- Load balancing
- Devices on the same subnet

3.6 Given a scenario, troubleshoot basic network connectivity issues.

- Tools
  - ping
  - tracert/traceroute
  - telnet
  - netstat
  - nslookup/dig
  - ipconfig/ifconfig
  - route
  - arp
- Review documentation and device configuration settings
- Review system logs

3.7 Explain common network protocols, ports and topologies.

- Trunk ports
- Port binding/aggregation
- Common ports
  - 80
  - 21
  - 22
  - 25
  - 53
  - 443
  - 68
- Common protocols
  - HTTP
  - FTP
  - HTTPS
  - FTPS
  - SFTP
  - SSH
  - DNS
  - DHCP
  - SMTP
- Types of networks
  - Intranet
  - Extranet
  - Internet

3.8 Explain common hardware resources and features used to enable virtual environments.

- BIOS/firmware configurations
- Minimum memory capacity and configuration
- Number of CPUs
- Number of cores
- NICs quantity, speeds and configurations
- Internal hardware compatibility
- HBAs
- Storage media
  - Tape
  - SSD
  - USB
  - Disk

4.0 Resource Management

4.1 Given a scenario, implement and use proper resource monitoring techniques.

- **Protocols**
  - SNMP
  - WMI
  - IPMI
  - Syslog service
- **Alert methods**
  - SMTP
  - SMS
  - SNMP
  - Web services
  - Syslog
- **Establish baselines and thresholds**
- **Automated responses to specific events**
- **Examine processes usage/resource usage**

4.2 Given a scenario, appropriately allocate physical (host) resources using best practices.

- **Memory**
- **CPU**
- **Storage and network allocation**
- **Entitlement/quotas (shares)**
  - Hard limit
  - Soft limit
- **Reservations**
- **Licensing**
- **Resource pooling**

4.3 Given a scenario, appropriately allocate virtual (guest) resources using best practices.

- **Virtual CPU**
- **Memory**
- **Storage and network allocation**
- **Entitlement/quotas (shares)**
- **Hard limit/soft limit**
- **Reservations/licensing**
- **Dynamic resource allocation**
- **Resource pooling**
- **CPU affinity**
- **Physical resource redirection and mapping to virtual resources**
  - Serial
  - USB
  - Parallel port mapping

4.4 Given a scenario, use appropriate tools for remote access.

- **Remote hypervisor access**
- **RDP**
- **SSH**
- **Console port**
- **HTTP**

5.0 Security

5.1 Explain network security concepts, tools and best practices.

- ACLs
- VPNs
- IDS/IPS hardware/ software-based firewalls
- DMZ
- Review/audit logs
- Attacks
  - DDoS
  - Ping of death
  - Ping flood

5.2 Explain storage security concepts, methods and best practices.

- Obfuscation
- Access control lists
- Zoning
- LUN masking
- User and host authentication
- Review/audit logs

5.3 Compare and contrast different encryption technologies and methods.

- PKI
- IPSec
- SSL/TLS
- Ciphers
  - AES
  - 3DES
  - RSA
  - DSA
  - RC4
  - RC5
- Encryption for data in transit and encryption for data at rest

5.4 Identify access control methods.

- Role-based administration
- Mandatory access controls
- Discretionary access controls
- Multifactor authentication
- Single sign-on
- Federation

5.5 Implement guest and host hardening techniques.

- Disabling unneeded ports and services
- User credentials
  - Changing default passwords
- Host-based/software firewalls
- Antivirus software
- Patching
- Deactivating default accounts

6.0 Systems Management

6.1 Explain policies and procedures as they relate to a cloud environment.

- **Network and IP planning/documentation**
- **Configuration standardization and documentation**
- **Change management best practices**
  - Documentation
  - Configuration control
  - Asset accountability
  - Approval process
  - Backout plan
- **Configuration management**
  - CMDB
  - Approval process
  - Configuration control
- **Capacity management**
  - Monitoring for changes
  - Trending
- **Systems life cycle management**
- **Maintenance windows**
  - Server upgrades and patches

6.2 Given a scenario, diagnose, remediate and optimize physical host performance.

- **Disk performance**
- **Disk tuning**
- **Disk latency**
- **Swap disk space**
- **I/O tuning**
- **Performance management and monitoring tools**
- **Establish baseline and create documentation with appropriate tools**
- **Hypervisor configuration best practices**
  - Memory ballooning
  - I/O throttling
  - CPU wait time
- **Impact of configuration changes to the virtual environment**
- **Common issues**
  - Disk failure
  - HBA failure
  - Memory failure
  - NIC failure
  - CPU failure

6.3 Explain common performance concepts as they relate to the host and the guest.

- **IOPS**
- **Read vs. write files**
- **File system performance**
- **Metadata performance**
- **Caching**
- **Bandwidth**
- **Throughput (bonding/teaming)**
- **Jumbo frames**
- **Network latency**
- **Hop counts**
- **QoS**
- **Multipathing**
- **Load balancing**
- **Scaling**
  - Vertical vs. horizontal vs. diagonal

6.4 Implement appropriate testing techniques when deploying cloud services.

- **Test replication**
- **Test latency**
- **Test bandwidth**
- **Test load balancing**
- **Test application servers**
- **Test storage**
- **Test application delivery**
- **Service performance testing and application performance testing**
- **Penetration testing**
- **Vulnerability assessment**
- **Separation of duties during testing**

7.0 Business Continuity in the Cloud

7.1 Compare and contrast disaster recovery methods and concepts.

- **Redundancy**
- **Failover**
- **Geographical diversity**
- **Failback**
- **Replication**
- **Site mirroring**
- **Hot site**
- **Cold site**
- **Warm site**
- **Backup and recovery**
- **Archiving and off-site storage**
- **Replication types**
  - Synchronous
  - Asynchronous
- **RTO**
- **RPO**
- **MTBF**
- **MTTR**
- **Mission-critical requirements**

7.2 Deploy solutions to meet availability requirements.

- **Fault tolerance**
  - High availability
  - Local clustering/geoclustering
  - Non-high-availability resources
- **Multipathing**
- **Load balancing**

CompTIA Cloud+ Acronyms

The following is a list of acronyms that appear on the CompTIA Cloud+ exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as a part of a comprehensive exam preparation program.

ACRONYM	SPELLED OUT
ACL	Access Control List
AES	Advanced Encryption Standard
API	Application Programming Interface
APM	Application Performance Monitor
ARP	Address Resolution Protocol
ASLR	Address Space Layout Randomization
ATA	Advanced Technology Attachment
BCP	Bridge Control Protocol
BGP	Border Gateway Protocol
BIA	Business Impact Analysis
BIOS	Basic Input/Output System
BMR	Bare Metal Restore
BPaaS	Business Process as a Service
BUN	Backup Network
C2C	Cloud to Cloud
C2D	Cloud to Database
CaaS	Communication as a Service or Computing as a Service
CAB	Change Advisory Board
CAN	Campus Area Network
CAS	Content Addressed Storage
CHAP	Challenge Handshake Application Protocol
CIFS	Common Internet File System
CIIS	Client Integration Implementation Service
CMDB	Configuration Management Database
CMS	Content Management System
CNA	Converged Network Adapter
COLO	Co-Location
COOP	Continuity Of Operations Plan
CPU	Central Processing Unit
CRL	Certificate Revocation List
CRM	Customer Relationship Management
CSP	Content Service Provider
D2C	Datacenter to Cloud
DaaS	Data as a Service

ACRONYM	SPELLED OUT
DAC	Discretionary Access Control
DAS	Direct Attached Storage
DBaaS	Database as a Service
DBMS	Database Management Server
DCB	Datacenter Bridging
DES	Data Encryption Standard
DFS	Distributed File System
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual In-line Memory Module
DLL	Dynamic Link Library
DMZ	Demilitarized Zone
DNS	Domain Name Service
DRP	Disaster Recovery Plan
DSA	Distributed Services Architecture
FAT	File Allocation Table
FC	Fibre Channel
FCIP	Fibre Channel over IP
FCoE	Fibre Channel over Ethernet
FTP	File Transfer Protocol
FTPS	FTP over SSL
GPT	GUID Partition Table
GUI	Graphical User Interface
HA	High Availability
HAV	Hardware-Assisted Virtualization
HBA	Host Bus Adapter
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
ICMP	Internet Control Management Protocol
IDE	Integrated Development Environment
IDS	Intrusion Detection System
IFCP	Internet Fibre Channel Protocol
IGRP	Interior Gateway Routing Protocol
IOPS	Input/Output Operations Per Second
IPC	Instructions Per Cycle
IPMI	Intelligent Platform Management Interface

ACRONYM	SPELLED OUT
IPS	Intrusion Protection system
IQN	Initiator Qualified Name
iSCSI	Internet SCSI
ISNS	Internet Storage Name Service
ISP	Internet Service Provider
JBOD	Just a Bunch Of Disks
KVM	Keyboard Video Mouse
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LUN	Logical Unit Number
MAC	Mandatory Access Control
MAN	Metropolitan Area Network
MBR	Master Boot Record
MDF	Main Distribution Facility
MPIO	Multipath I/O
MPLS	Multiprotocol Label Switching
MSP	Managed Service Provider
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
MTTR	Mean Time To Recovery
MTU	Maximum Transmission Unit
NAS	Network Attached Storage
NAT	Network Address Translation
NFS	Network File System
NIC	Network Interface Controller
NIS	Network Information Service
NNTP	Network News Transport Protocol
NOC	Network Operations Center
NPIV	N_Port ID Virtualization
NTFS	New Technology File System
ODBC	Open Database Connectivity
OLA	Operational-Level Agreement
OS	Operating System
OSD	Object Storage Device
OSPF	Open Shortest Path First
P2P	Physical to Physical
P2V	Physical to Virtual
PaaS	Platform as a Service
PAT	Port Address Translation
PBX	Public Branch Exchange
PIT	Point-In-Time (backup or snapshot)
PKI	Public Key Infrastructure
QoS	Quality of Service
QA	Quality Assurance
RAID	Redundant Array of Inexpensive Disks
RBAC	Role-Based Access Control

ACRONYM	SPELLED OUT
RDP	Remote Desktop Protocol
ReFS	Resilient File System
RIP	Routing Information Protocol
RPO	Recovery Point Objective
RTO	Recovery Time Objectives
SaaS	Software as a Service
SAN	Storage Area Network
SAS	Serial Attached SCSI
SATA	Serial ATA
SCP	Session Control Protocol
SCSI	Small Computer System Interface
SDLC	Software Development Life Cycle
SFTP	Secure FTP
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SSD	Solid State Disk
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On
TCO	Total Cost of Operations
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
TTD	Technical Training Device
TTL	Time To Live
UAT	Universal Access Transceiver
UDP	Universal Diagram Protocol
UPS	Universal Power Supply
UTA	Universal Target Adapter
V2P	Virtual to Physical
V2V	Virtual to Virtual
VAT	Virtual Allocation Table
VCPU	Virtual CPU
VDI	Virtual Desktop Infrastructure
VHD	Virtual Hard Disk
VLAN	Virtual LAN
VM	Virtual Machine
VMFS	Virtual Machine File System
VNC	Virtual Network Computing
VNIC	Virtual NIC
VPN	Virtual Private Network
VRAM	Virtual RAM
VSAN	Virtual SAN

ACRONYM	SPELLED OUT
Vswitch	Virtual Switch
VTL	Virtual Tape Library
WAN	Wide Area Network
WMI	Windows Management Implementation
WWNN	WorldWide Node Name
WWPN	WorldWide Port Name
WWUI	WorldWide Unique Identifier
XaaS	Anything as a Service
ZFS	Z File System

Cloud+ Proposed Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the Cloud+ exam. This list may also be helpful for training companies who wish to create a lab component to their training offering. The bulleted lists below each topic are a sample list and not exhaustive.

EQUIPMENT

- Router
- Firewall
- SAN/NAS/DAS/HBA
- At least two servers
- Multiple PCs
- Switch
- Tablets/PDAs/phones

SPARE PARTS/HARDWARE

- Keyboard, mouse, monitors
- CAT6
- Spare drives
- Spare bare-metal servers
- Fiber cable
- Spare HBA
- Spare CD/DVDs

TOOLS

- Screwdrivers
- Crimping tool
- Network sniffer
- Server administrative software tools

SOFTWARE

- Network sniffer
- Port scanner
- Hypervisor (Type I, Type II)
- Client and server OS
- Various Internet browsers
- Hypervisor management software
- Database software
- Network management software

OTHER

- Internet access
- Remote access to cloud service providers (free services)
- Administrative tools (admin pack)
- Self-service provisioning portal

CompTIA