CompTIA Cloud+ Certification Exam Objectives

EXAM NUMBER: CV0-003

About the Exam

Candidates are encouraged to use this document to help prepare for the CompTIA Cloud+ (CV0-003) certification exam. The CompTIA Cloud+ certification exam will verify the successful candidate has the knowledge and skills required to:

- **Understand cloud architecture and design**
- **Deploy cloud services and solutions**
- **Successfully maintain, secure, and optimize a cloud environment**
- **Troubleshoot common issues related to cloud management**

This is equivalent to 2—3 years of hands-on experience working in a systems administrator job role.

These content examples are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination.

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an 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 testing exam objectives. Please know that all related exam preparation materials will still be valid.

TEST DETAILS

Required exam	CV0-003
Number of questions	Maximum of 90
Types of questions	Multiple choice and performance-based
Length of test	90 minutes
Recommended experience	• At least 2—3 years of work experience in IT systems administration or IT networking • CompTIA Network+ and Server+ or equivalent knowledge • Familiarity with any major hypervisor technology for server virtualization • Knowledge of cloud service models • Knowledge of IT service management • Hands-on experience with at least one public or private cloud IaaS platform
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 Architecture and Design	13%
2.0 Security	20%
3.0 Deployment	23%
4.0 Operations and Support	22%
5.0 Troubleshooting	22%
Total	**100%**

1.0 Cloud Architecture and Design

1.1 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**

1.2 Explain the factors that contribute to capacity planning.

- **Requirements**
  - Hardware
  - Software
  - Budgetary
  - Business need analysis
- **Standard templates**
- **Licensing**
  - Per-user
  - Socket-based
  - Volume-based
  - Core-based
  - Subscription
- **User density**
- **System load**
- **Trend analysis**
  - Baselines
  - Patterns
  - Anomalies
- **Performance capacity planning**

1.3 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

1.4 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
        - Sizing
        - Subnetting
        - 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

2.0 Security

2.1 Given a scenario, configure identity and access management.

- **Identification and authorization**
  - Privileged access management
  - Logical access management
  - Account life-cycle management
    - Provision and deprovision accounts
  - Access controls
    - Role-based
    - Discretionary
    - Non-discretionary
    - 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**

2.2 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)
    - DNS over HTTPS (DoH)/ DNS over TLS (DoT)
    - DNS security (DNSSEC)
  - Network time protocol (NTP)
    - Network time security (NTS)
  - Encryption
    - IPSec
    - Transport layer security (TLS)
    - Hypertext transfer protocol secure (HTTPS)
  - Tunneling
    - Secure Shell (SSH)
    - Layer 2 tunneling protocol (L2TP)/ Point-to-point tunneling protocol (PPTP)
    - Generic routing encapsulation (GRE)
- **Network services**
  - Firewalls
    - Stateful
    - 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
    - Whitelisting or blacklisting
    - Proxy servers
  - Distributed denial of service (DDoS) protection

2.3 Given a scenario, apply the appropriate OS and application security controls.

- **Policies**
  - Password complexity
  - Account lockout
  - Application 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
- **Mandatory access control**
- **Software firewall**

2.4 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)**

2.5 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
- **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**

2.6 Explain the importance of incident response procedures.

- **Preparation**
  - Documentation
  - Call trees
  - Training
  - Tabletops
  - Documented incident types/categories
  - Roles and responsibilities
- **Incident response procedures**
  - Identification
    - Scope
  - Investigation
  - Containment, eradication, and recovery
    - Isolation
    - Evidence acquisition
    - Chain of custody
  - Post-incident and lessons learned
    - Root cause analysis

3.0 Deployment

3.1 Given a scenario, integrate components into a cloud solution.

- **Subscription services**
  - File subscriptions
  - Communications
    - Email
    - Voice over IP (VoIP)
    - Messaging
  - Collaboration
  - Virtual desktop infrastructure (VDI)
  - Directory and identity services
  - Cloud resources
    - IaaS
    - PaaS
    - 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**

3.2 Given a scenario, provision storage in cloud environments.

- **Types**
  - Block
    - Storage area network (SAN)
      - Zoning
  - File
    - Network attached storage (NAS)
  - Object
    - Tenants
    - 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)**

3.3 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
- **Virtual private cloud (VPC)**
  - Hub and spoke
  - Peering
- **VLAN/VXLAN/GENEVE**
- **Single root input/output virtualization (SR-IOV)**
- **Software-defined network (SDN)**

3.4 Given a scenario, configure the appropriate compute sizing for a deployment.

- **Virtualization**
  - Hypervisors
    - Type 1
    - Type 2
  - Simultaneous multi-threading (SMT)
  - Dynamic allocations
  - Oversubscription
- **Central processing unit (CPU)/ virtual CPU (vCPU)**
- **Graphics processing unit (GPU)**
  - Virtual
    - Shared
  - Pass-through
- **Clock speed/Instructions per cycle (IPC)**
- **Hyperconverged**
- **Memory**
  - Dynamic allocation
  - Ballooning

3.5 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
    - Access control lists (ACLs)
    - Firewalls
- **Storage migrations**
  - Block
  - File
  - Object
- **Database migrations**
  - Cross-service migrations
  - Relational
  - Non-relational

4.0 Operations and Support

4.1 Given a scenario, configure logging, monitoring, and alerting to maintain operational status.

- **Logging**
  - Collectors
    - Simple network management protocol (SNMP)
    - Syslog
  - Analysis
  - Severity categorization
  - Audits
  - Types
    - Access/authentication
    - System
    - Application
  - Automation
  - Trending
- **Monitoring**
  - Baselines
  - Thresholds
  - Tagging
  - Log scrubbing
  - Performance monitoring
    - Application
    - Infrastructure components
  - Resource utilization
  - Availability
    - SLA-defined uptime requirements
  - Verification of continuous monitoring activities
  - Service management tool integration
- **Alerting**
  - Common messaging methods
  - Enable/disable alerts
    - Maintenance mode
  - Appropriate responses
  - Policies for categorizing and communicating alerts

4.2 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
    - Hypervisors
    - VMs
    - Virtual appliances
    - Networking components
    - Applications
    - Storage components
    - Firmware
    - Software
    - OS
  - Policies
    - 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
    - Chargebacks
    - Showbacks
  - Elasticity usage
  - Connectivity
  - Latency
  - Capacity
  - Incidents
  - Health
  - Overall utilization
  - Availability

4.3 Given a scenario, optimize cloud environments.

- **Right-sizing**
  - Auto-scaling
  - Horizontal scaling
  - Vertical scaling
  - Cloud bursting
- **Compute**
  - CPUs
  - GPUs
  - Memory
  - Containers
- **Storage**
  - Tiers
    - Adaptive optimization
  - IOPS
  - Capacity
  - Deduplication
  - Compression
- **Network**
  - Bandwidth
  - Network interface controllers (NICs)
  - Latency
  - SDN
  - Edge computing
    - CDN
- **Placement**
  - Geographical
  - Cluster placement
  - Redundancy
  - Colocation
- **Device drivers and firmware**
  - Generic
  - Vendor
  - Open source

4.4 Given a scenario, apply proper automation and orchestration techniques.

- **Infrastructure as code**
  - Infrastructure components and their integration
- **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**

4.5 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
  - 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
    - Three copies of data
    - Two different media
    - One copy off site
- **Restoration methods**
  - In place
  - Alternate location
  - Restore files
  - Snapshot

4.6 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
  - Playbook
  - Network diagram
- **Geographical datacenter requirements**

5.0 Troubleshooting

5.1 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.

5.2 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
  - NAC
  - WAF
- **Unsupported protocols**
- **External/internal attacks**

5.3 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

5.4 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
    - Default
    - Static
    - Dynamic
  - Firewall
    - Incorrectly administered micro-segmentation
  - Network address translation (NAT)
    - VPN
    - Source
    - Destination
  - Load balancers
    - Methods
    - Headers
    - Protocols
    - Encryption
    - Back ends
    - 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
  - netstat/ss
  - route
  - arp
  - curl
  - Packet capture
  - Packet analyzer
  - OpenSSL client

5.5 Given a scenario, troubleshoot common performance issues.

- **Resource utilization**
  - CPU
  - GPU
  - Memory
  - Storage
    - I/O
    - Capacity
  - Network bandwidth
  - Network latency
  - Replication
  - Scaling
- **Application**
  - Memory management
  - Service overload
- **Incorrectly configured or failed load balancing**

5.6 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**

Cloud+ (CV0-003) Acronym List

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 part of a comprehensive exam preparation.

ACRONYM	DEFINITION
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
ADC	Application Delivery Controller
AES	Advanced Encryption Standard
AI	Artificial Intelligence
API	Application Programming Interface
ARP	Address Resolution Protocol
BCP	Business Continuity Plan
BGP	Border Gateway Protocol
BIA	Business Impact Analysis
CAB	Change Advisory Board
CAS	Content Addressed Storage
CASB	Cloud Access Security Broker
CD	Continuous Deployment
CDN	Content Delivery Network
CI	Continuous Integration
CIFS	Common Internet File System
CIIS	Client Integration Implementation Service
CMDB	Configuration Management Database
CMS	Content Management System
CNA	Converged Network Adapter
COL	Co-Location
COOP	Continuity of Operations Plan
CPU	Central Processing Unit
CRL	Certificate Revocation List
CRM	Customer Relationship Management
CSP	Content Service Provider
DAC	Discretionary Access Control
DAS	Direct Attached Storage
DBaaS	Database as a Service
DBMS	Database Management Server
DDoS	Distributed Denial of Service
DFS	Distributed File System
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNS	Domain Name Service
DNSSEC	DNS Security
DoH	DNS over HTTPS
DoT	DNS over TLS
DR	Disaster Recovery
DRP	Disaster Recovery Plan
DSA	Distributed Services Architecture
EDR	Endpoint Detection and Response
FC	Fibre Channel
FCoE	Fibre Channel over Ethernet
FIM	File Integrity Monitoring
FTP	File Transfer Protocol
FTPS	FTP over SSL
GENEVE	Generic Network Virtualization Encapsulation
GPT	GUID Partition Table
GPU	Graphics Processing Unit
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
HA	High Availability
HBA	Host Bus Adapter
HIDS	Host-Based IDS
HIPS	Host-Based IPS
HTTPS	Hypertext Transfer Protocol Secure
I/O	Input/Output
IaaS	Infrastructure as a Service
ICMP	Internet Control Management Protocol
IDS	Intrusion Detection System
IFCP	Internet Fibre Channel Protocol
IGRP	Interior Gateway Routing Protocol
IOPS	Input/Output Operations Per Second
IoT	Internet of Things
IPAM	IP Address Management
IPC	Instructions Per Cycle
IPMI	Intelligent Platform Management Interface
IPS	Intrusion Prevention System

ACRONYM	DEFINITION
IPSec	IP Security
IQN	Initiator Qualified Name
iSCSI	Internet Small Computer System Interface
ISNS	Internet Storage Name Service
ISP	Internet Service Provider
JBOD	Just a Bunch Of Disks
KVM	Kernel Virtual Machine
KVM	Keyboard Video Mouse
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LTS	Long Term Support
LUN	Logical Unit Number
MAC	Mandatory Access Control
MBR	Master Boot Record
MDF	Main Distribution Facility
MFA	Multi-Factor Authentication
ML	Machine Learning
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 Repair
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAS	Network Attached Storage
NAT	Network Address Translation
NFS	Network File System
NIC	Network Interface Controller
NIS	Network Information Service
NOC	Network Operations Center
NPIV	N_Port ID Virtualization
NTFS	New Technology File System
NTP	Network Time Protocol
NTS	Network Time Security
NVMe	Non-Volatile Memory Express
NVMe-oF	NVMe over Fabrics
ODBC	Open Database Connectivity
OLA	Operational Level Agreement
OS	Operating System
OSPF	Open Shortest Path First
P2P	Physical to Physical
P2V	Physical to Virtual
PaaS	Platform as a Service
PAT	Port Address Translation
PBX	Private (or Public) Branch Exchange
PIT	Point-in-Time (backup or snapshot)
PKI	Public Key Infrastructure
PPTP	Point-to-point Tunneling Protocol
QA	Quality Assurance
QoS	Quality of Service
RAID	Redundant Array of Inexpensive Disks
RDP	Remote Desktop Protocol
ReFS	Resilient File System
RPO	Recovery Point Objective
RTO	Recovery Time Objectives
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAN	Storage Area Network
SAS	Serial Attached SCSI
SATA	Serial Advanced Technology Attachment
SCP	Session Control Protocol
SCSI	Small Computer System Interface
SDLC	Software Development Life Cycle
SDN	Software-Defined Network
SDS	Software-Defined Storage
SFTP	Secure FTP
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMB	Server Message Block
SMT	Simultaneous Multi-Threading
SNMP	Simple Network Management Protocol
SR-IOV	Single-Root Input/ Output Virtualization
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
TTL	Time to Live
UAT	User Acceptance Testing
UDP	Universal Datagram Protocol
UPS	Universal Power Supply
V2P	Virtual to Physical
V2V	Virtual to Virtual
VAT	Virtual Allocation Table
vCPU	Virtual CPU
VDI	Virtual Desktop Infrastructure
vGPU	Virtual Graphics Processing Unit

ACRONYM	DEFINITION
VHD	Virtual Hard Disk
VLAN	Virtual LAN
VM	Virtual Machine
VMFS	Virtual Machine File System
VNC	Virtual Network Computing
vNIC	Virtual NIC
VoIP	Voice over IP
VPC	Virtual Private Cloud
VPN	Virtual Private Network
vRAM	Virtual RAM
vSAN	Virtual SAN
vSwitch	Virtual Switch
VTL	Virtual Tape Library
VXLAN	Virtual extensible LAN
WAF	Web Application Firewall
WAN	Wide Area Network
WMI	Windows Management Implementation
WWNN	World Wide Node Name
WWPN	World Wide Port Name
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 that wish to create a lab component to their training offering. The bulleted lists below each topic are sample lists and are not exhaustive.

HARDWARE

- Computer capable of running virtualization
- Network switch**
- Network router**
- Compute (CPU, RAM, etc.)**
- NAS or SAN**
- Cables**

SOFTWARE

- Automation tools
- Hypervisor (Type 1, Type 2)
- Client (and server) OS
- Various web browsers
- CLI**
- Virtualization format converter**

OTHER

- Internet access
- Access to SaaS, PaaS, or IaaS environments
- Remote access to cloud service providers (trial or free service)

**Ideal, but not necessary for lab setup