CompTIA Cloud+ Certification Exam Objectives

EXAM NUMBER: CV0-002

CompTIA

About the Exam

The CompTIA Cloud+ certification is an internationally recognized validation of the knowledge required of IT practitioners working in cloud computing environments. The CompTIA Cloud+ CV0-002 exam will certify the successful candidate has the knowledge and skills required to:

- **Understand standard cloud methodologies**
- **Implement, maintain and deliver cloud technologies (e.g., network, storage and virtualization technologies**
- **Understand aspects of IT security and use industry best practices related to cloud implementations**

It is recommended that CompTIA Cloud+ candidates have the following:

- **CompTIA Network+ certification and/or CompTIA Server+ certification, although CompTIA certifications are not required**
- **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, although vendor-specific certifications in virtualization are not required**
- **Knowledge of cloud service model (IaaS, Paas, Saas) definitions**
- **Knowledge of common cloud deployment model (private, public, hybrid) definitions**
- **Hands-on experience with at least one public cloud IaaS platform**

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	CV0-002
Number of questions	Maximum of 90
Type of questions	Multiple choice and performance-based
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 • Knowledge of cloud service model (IaaS, PaaS, SaaS) definitions • Knowledge of common cloud deployment model (Private, Public, Hybrid) definitions • Hands-on experience with at least one public 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 Configuration and Deployment	24%
2.0 Security	16%
3.0 Maintenance	18%
4.0 Management	20%
5.0 Troubleshooting	22%
Total	**100%**

1.0 Configuration and Deployment

1.1 Given a scenario, analyze system requirements to ensure successful system deployment.

- **Appropriate commands, structure, tools, and automation/orchestration as needed**
- **Platforms and applications**
- **Interaction of cloud components and services**
  - Network components
  - Application components
  - Storage components
  - Compute components
  - Security components
- **Interaction of non-cloud components and services**
- **Baselines**
- **Target hosts**
- **Existing systems**
- **Cloud architecture**
- **Cloud elements/target objects**

1.2 Given a scenario, execute a provided deployment plan.

- **Apply the change management process**
  - Approvals
  - Scheduling
- **Refer to documentation and follow standard operating procedures**
- **Execute workflow**
- **Configure automation and orchestration, where appropriate, for the system being deployed**
- **Use commands and tools as needed**
- **Document results**

1.3 Given a scenario, analyze system requirements to determine if a given testing plan is appropriate.

- **Underlying environmental considerations included in the testing plan**
  - Shared components
    - Storage
    - Compute
    - Network
  - Production vs. development vs. QA
  - Sizing
  - Performance
  - High availability
  - Connectivity
  - Data integrity
  - Proper function
  - Replication
  - Load balancing
  - Automation/orchestration
- **Testing techniques**
  - Vulnerability testing
  - Penetration testing
  - Load testing

1.4 Given a scenario, analyze testing results to determine if the testing was successful in relation to given system requirements.

- **Consider success factor indicators of the testing environment**
  - Sizing
  - Performance
  - Availability
  - Connectivity
  - Data integrity
  - Proper functionality
- **Document results**
- **Baseline comparisons**
- **SLA comparisons**
- **Cloud performance fluctuation variables**

1.5 Given a scenario, analyze sizing, subnetting, and basic routing for a provided deployment of the virtual network.

- **Cloud deployment models**
  - Public
  - Private
  - Hybrid
  - Community
- **Network components**
- **Applicable port and protocol considerations when extending to the cloud**
- **Determine configuration for the applicable platform as it applies to the network**
  - VPN
  - IDS/IPS
  - DMZ
  - VXLAN
  - Address space required
  - Network segmentation and microsegmentation
- **Determine if cloud resources are consistent with the SLA and/or change management requirements**

1.6 Given a scenario, analyze CPU and memory sizing for a provided deployment.

- **Available vs. proposed resources**
  - CPU
  - RAM
- **Memory technologies**
  - Bursting and ballooning
  - Overcommitment ratio
- **CPU technologies**
  - Hyperthreading
  - VT-x
  - Overcommitment ratio
- **Effect to HA/DR**
- **Performance considerations**
- **Cost considerations**
- **Energy savings**
- **Dedicated compute environment vs. shared compute environment**

1.7 Given a scenario, analyze the appropriate storage type and protection capability for a provided deployment.

- **Requested IOPS and read/write throughput**
- **Protection capabilities**
  - High availability
    - Failover zones
  - Storage replication
    - Regional
    - Multiregional
    - Synchronous and asynchronous
  - Storage mirroring
  - Cloning
  - Redundancy level/factor
- **Storage types**
  - NAS
  - DAS
  - SAN
  - Object storage
- **Access protocols**
- **Management differences**
- **Provisioning model**
  - Thick provisioned
  - Thin provisioned
  - Encryption requirements
  - Tokenization
- **Storage technologies**
  - Deduplication technologies
  - Compression technologies
- **Storage tiers**
- **Overcommitting storage**
- **Security configurations for applicable platforms**
  - ACLs
  - Obfuscation
  - Zoning
  - User/host authentication and authorization

1.8 Given a scenario, analyze characteristics of the workload (storage, network, compute) to ensure a successful migration.

- **Migration types**
  - P2V
  - V2V
  - V2P
  - P2P
  - Storage migrations
  - Online vs. offline migrations
- **Source and destination format of the workload**
  - Virtualization format
  - Application and data portability
- **Network connections and data transfer methodologies**
- **Standard operating procedures for the workload migration**
- **Environmental constraints**
  - Bandwidth
  - Working hour restrictions
  - Downtime impact
  - Peak timeframes
  - Legal restrictions
  - Follow-the-sun constraints/time zones

1.9 Given a scenario, apply elements required to extend the infrastructure into a given cloud solution.

- **Identity management elements**
  - Identification
  - Authentication
  - Authorization
    - Approvals
    - Access policy
  - Federation
    - Single sign-on
- **Appropriate protocols given requirements**
- **Element considerations to deploy infrastructure services such as:**
  - DNS
  - DHCP
  - Certificate services
  - Local agents
  - Antivirus
  - Load balancer
  - Multifactor authentication
  - Firewall
  - IPS/IDS

2.0 Security

2.1 Given a scenario, apply security configurations and compliance controls to meet given cloud infrastructure requirements.

- **Company security policies**
- **Apply security standards for the selected platform**
- **Compliance and audit requirements governing the environment**
  - Laws and regulations as they apply to the data
- **Encryption technologies**
  - IPSec
  - SSL/TLS
  - Other ciphers
- **Key and certificate management**
  - PKI
- **Tunneling protocols**
  - L2TP
  - PPTP
  - GRE
- **Implement automation and orchestration processes as applicable**
- **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

2.2 Given a scenario, apply the appropriate ACL to the target objects to meet access requirements according to a security template.

- **Authorization to objects in the cloud**
  - Processes
  - Resources
    - Users
    - Groups
    - System
      - Compute
      - Networks
      - Storage
  - Services
- **Effect of cloud service models on security implementations**
- **Effect of cloud deployment models on security implementations**
- **Access control methods**
  - Role-based administration
  - Mandatory access controls
  - Discretionary access controls
  - Non-discretionary access controls
  - Multifactor authentication
  - Single sign-on

2.3 Given a cloud service model, implement defined security technologies to meet given security requirements.

- **Data classification**
- **Concepts of segmentation and microsegmentation**
  - Network
  - Storage
  - Compute
- **Use encryption as defined**
- **Use multifactor authentication as defined**
- **Apply defined audit/ compliance requirements**

2.4 Given a cloud service model, apply the appropriate security automation technique to the target system.

- **Tools**
  - APIs
  - Vendor applications
  - CLI
  - Web GUI
  - Cloud portal
- **Techniques**
  - Orchestration
  - Scripting
  - Custom programming
- **Security services**
  - Firewall
  - Antivirus/anti-malware
  - IPS/IDS
  - HIPS
- **Impact of security tools to systems and services**
  - Scope of impact
- **Impact of security automation techniques as they relate to the criticality of systems**
  - Scope of impact

3.0 Maintenance

3.1 Given a cloud service model, determine the appropriate methodology to apply given patches.

- **Scope of cloud elements to be patched**
  - Hypervisors
  - Virtual machines
  - Virtual appliances
  - Networking components
  - Applications
  - Storage components
  - Clusters
- **Patching methodologies and standard operating procedures**
  - Production vs. development vs. QA
  - Rolling update
  - Blue-green deployment
  - Failover cluster
- **Use order of operations as it pertains to elements that will be patched**
- **Dependency considerations**

3.2 Given a scenario, apply the appropriate automation tools to update cloud elements.

- **Types of updates**
  - Hotfix
  - Patch
  - Version update
  - Rollback
- **Automation workflow**
  - Runbook management
    - Single node
    - Orchestration
      - Multiple nodes
      - Multiple runbooks
- **Activities to be performed by automation tools**
  - Snapshot
  - Cloning
  - Patching
  - Restarting
  - Shut down
  - Maintenance mode
  - Enable/disable alerts

3.3 Given a scenario, apply an appropriate backup or restore method.

- **Backup types**
  - Snapshot/redirect-on-write
  - Clone
  - Full
  - Differential
  - Incremental
  - Change block/delta tracking
- **Backup targets**
  - Replicas
  - Local
  - Remote
- **Other considerations**
  - SLAs
  - Backup schedule
  - Configurations
  - Objects
  - Dependencies
  - Online/offline

3.4 Given a cloud-based scenario, apply appropriate disaster recovery methods.

- **DR capabilities of a cloud service provider**
- **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

3.5 Given a cloud-based scenario, apply the appropriate steps to ensure business continuity.

- **Business continuity plan**
  - Alternate sites
  - Continuity of operations
  - Connectivity
  - Edge sites
  - Equipment
  - Availability
  - Partners/third parties
- **SLAs for BCP and HA**

3.6 Given a scenario, apply the appropriate maintenance automation technique to the target objects.

- **Maintenance schedules**
- **Impact and scope of maintenance tasks**
- **Impact and scope of maintenance automation techniques**
- **Include orchestration as appropriate**
- **Maintenance automation tasks**
  - Clearing logs
  - Archiving logs
  - 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

4.0 Management

4.1 Given a scenario, analyze defined metrics to determine the presence of an abnormality and/or forecast future needed cloud resources.

- **Monitoring**
  - Target object baselines
  - Target object anomalies
  - Common alert methods/messaging
  - Alerting based on deviation from baseline
  - Event collection
- **Event correlation**
- **Forecasting resource capacity**
  - Upsize/increase
  - Downsize/decrease
- **Policies in support of event collection**
- **Policies to communicate alerts appropriately**

4.2 Given a scenario, determine the appropriate allocation of cloud resources.

- **Resources needed based on cloud deployment models**
  - Hybrid
  - Community
  - Public
  - Private
- **Capacity/elasticity of cloud environment**
- **Support agreements**
  - Cloud service model maintenance responsibility
- **Configuration management tool**
- **Resource balancing techniques**
- **Change management**
  - Advisory board
  - Approval process
  - Document actions taken
    - CMDB
    - Spreadsheet

4.3 Given a scenario, determine when to provision/deprovision cloud resources.

- **Usage patterns**
- **Cloud bursting**
  - Auto-scaling technology
- **Cloud provider migrations**
- **Extending cloud scope**
- **Application life cycle**
  - Application deployment
  - Application upgrade
  - Application retirement
  - Application replacement
  - Application migration
  - Application feature use
    - Increase/decrease
- **Business need change**
  - Mergers/acquisitions/divestitures
  - Cloud service requirement changes
  - Impact of regulation and law changes

4.4 Given a scenario, implement account provisioning techniques in a cloud environment to meet security and policy requirements.

- **Identification**
- **Authentication methods**
  - Federation
    - Single sign-on
- **Authorization methods**
  - ACLs
  - Permissions
- **Account life cycle**
- **Account management policy**
  - Lockout
  - Password complexity rules
- **Automation and orchestration activities**
  - User account creation
  - Permission settings
  - Resource access
  - User account removal
  - User account disablement

4.5 Given a scenario, analyze deployment results to confirm they meet the baseline.

- **Procedures to confirm results**
  - CPU usage
  - RAM usage
  - Storage utilization
  - Patch versions
  - Network utilization
  - Application version
  - Auditing enable
  - Management tool compliance

4.6 Given a specific environment and related data (e.g., performance, capacity, trends), apply appropriate changes to meet expected criteria.

- **Analyze performance trends**
- **Refer to baselines**
- **Refer to SLAs**
- **Tuning of cloud target objects**
  - Compute
  - Network
  - Storage
  - Service/application resources
- **Recommend changes to meet expected performance/capacity**
  - Scale up/down (vertically)
  - Scale in/out (horizontally)

4.7 Given SLA requirements, determine the appropriate metrics to report.

- **Chargeback/showback models**
  - Reporting based on company policies
  - Reporting based on SLAs
- **Dashboard and reporting**
  - Elasticity usage
  - Connectivity
  - Latency
  - Capacity
  - Overall utilization
  - Cost
  - Incidents
  - Health
  - System availability
    - Uptime
    - Downtime

5.0 Troubleshooting

5.1 Given a scenario, troubleshoot a deployment issue.

- **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

5.2 Given a scenario, troubleshoot common capacity issues.

- **Exceeded cloud capacity boundaries**
  - Compute
  - Storage
  - Networking
    - IP address limitations
    - Bandwidth limitations
  - Licensing
  - Variance in number of users
  - API request limit
  - Batch job scheduling issues
- **Deviation from original baseline**
- **Unplanned expansions**

5.3 Given a scenario, troubleshoot automation/orchestration issues.

- **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

5.4 Given a scenario, troubleshoot connectivity issues.

- **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
- **Network tool outputs**
- **Network connectivity tools**
  - ping
  - tracert/traceroute
  - telnet
  - netstat
  - nslookup/dig
  - ipconfig/ifconfig
  - route
  - arp
  - ssh
  - tcpdump
- **Remote access tools for troubleshooting**

5.5 Given a scenario, troubleshoot security issues.

- **Authentication issues**
  - Account lockout/expiration
- **Authorization issues**
- **Federation and single sign-on issues**
- **Certificate expiration**
- **Certification misconfiguration**
- **External attacks**
- **Internal attacks**
- **Privilege escalation**
- **Internal role change**
- **External role change**
- **Security device failure**
- **Incorrect hardening settings**
- **Unencrypted communication**
- **Unauthorized physical access**
- **Unencrypted data**
- **Weak or obsolete security technologies**
- **Insufficient security controls and processes**
- **Tunneling or encryption issues**

5.6 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
   - 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 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 part of a comprehensive exam preparation program.

ACRONYM	SPELLED OUT
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
API	Application Programming Interface
APM	Application Performance Monitor
ARP	Address Resolution Protocol
BCP	Business Continuity Plan
BGP	Border Gateway Protocol
BIA	Business Impact Analysis
BLOB	Binary Large Object
BMR	Bare Metal Restore
BPaaS	Business Process as a Service
CAB	Change Advisory Board
CaaS	Communication as a Service/ Computing as a Service
CapEx	Capital Expenditures
CAS	Content Addressed Storage
CASB	Cloud Access Security Broker
CI/CD	Continuous Integration/Continuous Deployment
CIFS	Common Internet File System
CIIS	Client Integration Implementation Service
CLI	Command Line Interface
CMDB	Configuration Management Database
CM	Configuration Management
CMP	Cloud Management Platform
CMS	Content Management System
CNA-	Converged Network Adapter
CNAME	Canonical Name
COLO	Co-location
COOP	Continuity of Operations Plan
CPU	Central Processing Unit
CRL	Certificate Revocation List
CRM	Customer Relationship Management
CSA	Cloud Systems Administrator
CSP	Cloud Service Provider

ACRONYM	SPELLED OUT
DaaS	Desktop as a Service
DAC	Discretionary Access Control
DAS	Direct Attached Storage
DBA	Database Administrator
DBaaS	Database as a Service
DBMS	Database Management Server
DES	Data Encryption Standard
DFS	Distributed File System
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual In-line Memory Module
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNS	Domain Name Service
DR	Disaster Recovery
DRaaS	Disaster Recovery as a Service
DRP	Disaster Recovery Plan
DSA	Distributed Services Architecture
ECAB	Emergency Change Advisory Board
ECC	Elliptic Curve Cryptography
FAT	File Allocation Table
FC	Fibre Channel
FCIP	Fibre Channel over IP
FCoE	Fibre Channel over Ethernet
FIM	File Integrity Monitoring
FTP	File Transfer Protocol
FTPS	FTP over SSL
GPT	GUID Partition Table
GPU	Graphics Processing Unit
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
HA	High Availability
HBA	Host Bus Adapter
HDFS	Hadoop Distributed File System
HIPS	Host Intrusion Prevention System
HTTPS	Hypertext Transfer Protocol Secure

ACRONYM	SPELLED OUT
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
ICMP	Internet Control Management Protocol
IDP	Intrusion Detection and Prevention
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
IPS	Intrusion Protection System
IPSec	Internet Protocol Security
IQN	Initiator Qualified Name
IRM	Information Rights Management
ISP	Internet Service Provider
iSCSI	Internet Small Computer Systems Interface
ISNS	Internet Storage Name Service
ITIL	Information Technology Infrastructure Library
JBOD	Just a Bunch of Disks
JSON	JavaScript Object Notation
KMS	Key Management System
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
MBR	Master Boot Record
MDF	Main Distribution Facility
MFA	Multifactor Authentication
MPIO	Multipath Input/Output
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
NAC	Network Access Control
NAS	Network Attached Storage
NAT	Network Address Translation
NFS	Network File System
NFV	Network Function Virtualization
NIC	Network Interface Controller
NIS	Network Information Service
NOC	Network Operations Center
NPIV	N_Port ID Virtualization
NTFS	New Technology File System
NTLM	NT LAN Manager
NTP	Network Time Protocol
NVMe	Non-Volatile Memory Express
ODBC	Open Database Connectivity
OLA	Operational Level Agreement
OpEx	Operating Expenditure
OS	Operating System
OSPF	Open Shortest Path First
OVA	Open Virtual Appliance
OVF	Open Virtualization Format
P2P	Physical to Physical
P2V	Physical to Virtual
PaaS	Platform as a Service
PAC	Proxy Automatic Configuration
PAM	Pluggable Authentication Modules
PAT	Port Address Translation
PBX	Private (or Public) Branch Exchange
PCI	Payment Card Industry
PCS	Private Cloud Space
PII	Personally Identifiable Information
PIT	Point-in-Time
PKI	Public Key Infrastructure
PSK	Pre-Shared Key
QA	Quality Assurance
QoS	Quality of Service
RAID	Redundant Array of Inexpensive Disks
RBAC	Role-Based Access Control
RC5	Rivest Cipher 5
RDP	Remote Desktop Protocol
ReFS	Resilient File System
RIP	Routing Information Protocol
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SAML	Security Assertions 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
SED	Self-Encrypting Drive
SFTP	Secure FTP
SHA	Secure Hash Algorithm
SIEM	Security Incident Event Manager
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMB	Server Message Block

ACRONYM	SPELLED OUT
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedure
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	User Acceptance Testing
UDP	Universal Datagram 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
VMDK	Virtual Machine Disk
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
VRF	Virtual Routing and Forwarding
VRR	Vulnerability Remediation Request
VSAN	Virtual SAN
vSwitch	Virtual Switch
VTL	Virtual Tape Library
VXLAN	Virtual Extensible Local Area Network
WAF	Web Application Firewall
WAN	Wide Area Network
WMI	Windows Management Implementation
WWNN	World Wide Node Name
WWPN	World Wide Port Name
WWUI	World Wide 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 that wish to create a lab component for their training offering. The bulleted lists below each topic are sample lists and not exhaustive.

EQUIPMENT

- Hyperconverged infrastructure or system
  - Shared storage/hard drives
  - SAN switches
  - Backup service
  - Replication to cloud services
  - Virtual firewall
  - Compute (CPU, RAM, etc.)
- Switch for client PCs
- Router
- Access to SaaS, PaaS, IaaS environments
- Client PCs (laptops/desktops)

SPARE PARTS/HARDWARE

- Keyboard, mouse, monitors
- Cat 6

SOFTWARE

- Automation tools
- Hypervisor (Type 1, Type 2)
- Client and server OS
- Various Internet browsers
- Hypervisor management software
- Cloud 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