CompTIA Cloud+ Certification Exam Objectives

EXAM NUMBER: CV0-002
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+ exam will certify the successful candidate has the knowledge and skills required to understand standard cloud methodologies; to implement, maintain, and deliver cloud technologies (e.g., network, storage, and virtualization technologies); and to 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: 100
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:

<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>PERCENTAGE OF EXAMINATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Configuration and Deployment</td>
<td>24%</td>
</tr>
<tr>
<td>2.0 Security</td>
<td>16%</td>
</tr>
<tr>
<td>3.0 Maintenance</td>
<td>18%</td>
</tr>
<tr>
<td>4.0 Management</td>
<td>20%</td>
</tr>
<tr>
<td>5.0 Troubleshooting</td>
<td>22%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
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 environment 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
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

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 micro-segmentation
- Determine if cloud resources are consistent with the SLA and/or change management requirements

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

CompTIA Cloud+ Certification Exam Objectives Version 2.0 (Exam Number: CV0-002)
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
- Storage 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 micro-segmentation
  - Network
  - Storage
  - Compute
- Use encryption as defined
- Use multifactor authentication as defined
- Apply defined audit/compliance requirements
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
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

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

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
  - 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

CompTIA Cloud+ Certification Exam Objectives Version 2.0 (Exam Number: CV0-002)
4.0 Management

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

CompTIA Cloud+ Certification Exam Objectives Version 2.0 (Exam Number: CV0-002)
5.0 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.

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 a part of a comprehensive exam preparation program.

<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Authentication, Authorization, and Accounting</td>
<td>DAS</td>
<td>Direct Attached Storage</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control List</td>
<td>DBaaS</td>
<td>Database as a Service</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
<td>DBMS</td>
<td>Database Management Server</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>APM</td>
<td>Application Performance Monitor</td>
<td>DFS</td>
<td>Distributed File System</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Plan</td>
<td>DIMM</td>
<td>Dual In-line Memory Module</td>
</tr>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
<td>DMZ</td>
<td>Demilitarized Zone</td>
</tr>
<tr>
<td>BIA</td>
<td>Business Impact Analysis</td>
<td>DNS</td>
<td>Domain Name Service</td>
</tr>
<tr>
<td>BLOB</td>
<td>Binary Large Object</td>
<td>DRP</td>
<td>Disaster Recovery Plan</td>
</tr>
<tr>
<td>BMR</td>
<td>Bare Metal Restore</td>
<td>DSA</td>
<td>Distributed Services Architecture</td>
</tr>
<tr>
<td>BPaaS</td>
<td>Business Process as a Service</td>
<td>ECC</td>
<td>Elliptic Curve Cryptography</td>
</tr>
<tr>
<td>CAB</td>
<td>Change Advisory Board</td>
<td>FAT</td>
<td>File Allocation Table</td>
</tr>
<tr>
<td>CaaS</td>
<td>Communication as a Service/Computing as a Service</td>
<td>FC</td>
<td>Fibre Channel</td>
</tr>
<tr>
<td>CAS</td>
<td>Content Addressed Storage</td>
<td>FCIP</td>
<td>Fibre Channel over IP</td>
</tr>
<tr>
<td>CASB</td>
<td>Cloud Access Security Broker</td>
<td>FCoE</td>
<td>Fibre Channel over Ethernet</td>
</tr>
<tr>
<td>CI/CD</td>
<td>Continuous Integration/Continuous Deployment</td>
<td>FIM</td>
<td>File Integrity Monitoring</td>
</tr>
<tr>
<td>CIFS</td>
<td>Common Internet File System</td>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>CIIS</td>
<td>Client Integration Implementation Service</td>
<td>FTPS</td>
<td>FTP over SSL</td>
</tr>
<tr>
<td>CLI</td>
<td>Command Line Interface</td>
<td>GPT</td>
<td>GUID Partition Table</td>
</tr>
<tr>
<td>CMDB</td>
<td>Configuration Management Database</td>
<td>GRE</td>
<td>Generic Routing Encapsulation</td>
</tr>
<tr>
<td>CM</td>
<td>Configuration Management</td>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>CMP</td>
<td>Cloud Management Platform</td>
<td>HA</td>
<td>High Availability</td>
</tr>
<tr>
<td>CMS</td>
<td>Content Management System</td>
<td>HBA</td>
<td>Host Bus Adapter</td>
</tr>
<tr>
<td>CNA-</td>
<td>Converged Network Adapter</td>
<td>HDFS</td>
<td>Hadoop Distributed File System</td>
</tr>
<tr>
<td>CNAME</td>
<td>Canonical Name</td>
<td>HIPs</td>
<td>Host Intrusion Prevention System</td>
</tr>
<tr>
<td>COLO</td>
<td>Co-location</td>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>COOP</td>
<td>Continuity of Operations Plan</td>
<td>IaaS</td>
<td>Infrastructure as a Service</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
<td>IAM</td>
<td>Identity and Access Management</td>
</tr>
<tr>
<td>CRL</td>
<td>Certificate Revocation List</td>
<td>ICMP</td>
<td>Internet Control Management Protocol</td>
</tr>
<tr>
<td>CRM</td>
<td>Customer Relationship Management</td>
<td>IDP</td>
<td>Intrusion Detection and Prevention</td>
</tr>
<tr>
<td>CSA</td>
<td>Cloud Systems Administrator</td>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>CSP</td>
<td>Cloud Service Provider</td>
<td>IFCP</td>
<td>Internet Fibre Channel Protocol</td>
</tr>
<tr>
<td>DAC</td>
<td>Discretionary Access Control</td>
<td>IGRP</td>
<td>Interior Gateway Routing Protocol</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IOPS</td>
<td>Input/output Operations Per Second</td>
</tr>
</tbody>
</table>

CompTIA Cloud+ Certification Exam Objectives Version 2.0 (Exam Number: CV0-002)
<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPC</td>
<td>Instructions Per Cycle</td>
<td>PaaS</td>
<td>Platform as a Service</td>
</tr>
<tr>
<td>IPMI</td>
<td>Intelligent Platform Management Interface</td>
<td>PAC</td>
<td>Proxy Automatic Configuration</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Protection System</td>
<td>PAT</td>
<td>Port Address Translation</td>
</tr>
<tr>
<td>IQN</td>
<td>Initiator Qualified Name</td>
<td>PBX</td>
<td>Private (or Public) Branch Exchange</td>
</tr>
<tr>
<td>IRM</td>
<td>Information Rights Management</td>
<td>PCS</td>
<td>Private Cloud Space</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>iSCSI</td>
<td>Internet Small Computer Systems Interface</td>
<td>PIT</td>
<td>Point-in-Time</td>
</tr>
<tr>
<td>ISNS</td>
<td>Internet Storage Name Service</td>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>ITIL</td>
<td>Information Technology Infrastructure Library</td>
<td>PSK</td>
<td>Pre-Shared Key</td>
</tr>
<tr>
<td>JBOD</td>
<td>Just a Bunch of Disks</td>
<td>QA</td>
<td>Quality Assurance</td>
</tr>
<tr>
<td>JSON</td>
<td>JavaScript Object Notation</td>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>KMS</td>
<td>Key Management System</td>
<td>RAID</td>
<td>Redundant Array of Inexpensive Disks</td>
</tr>
<tr>
<td>KVM</td>
<td>Keyboard Video Mouse</td>
<td>RBAC</td>
<td>Role-Based Access Control</td>
</tr>
<tr>
<td>L2TP</td>
<td>Layer 2 Tunneling Protocol</td>
<td>RC5</td>
<td>Rivest Cipher 5</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
<td>RDP</td>
<td>Remote Desktop Protocol</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
<td>ReFS</td>
<td>Resilient File System</td>
</tr>
<tr>
<td>LUN</td>
<td>Logical Unit Number</td>
<td>RIP</td>
<td>Routing Information Protocol</td>
</tr>
<tr>
<td>MAC</td>
<td>Mandatory Access Control</td>
<td>RPO</td>
<td>Recovery Point Objective</td>
</tr>
<tr>
<td>MBR</td>
<td>Master Boot Record</td>
<td>RTO</td>
<td>Recovery Time Objective</td>
</tr>
<tr>
<td>MDF</td>
<td>Main Distribution Facility</td>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>MFA</td>
<td>Multifactor Authentication</td>
<td>SAML</td>
<td>Security Assertions Markup Language</td>
</tr>
<tr>
<td>MPIO</td>
<td>Multipath Input/Output</td>
<td>SAN</td>
<td>Storage Area Network</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multiprotocol Label Switching</td>
<td>SAS</td>
<td>Serial Attached SCSI</td>
</tr>
<tr>
<td>MSP</td>
<td>Managed Service Provider</td>
<td>SATA</td>
<td>Serial Advanced Technology Attachment</td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean Time Between Failure</td>
<td>SCP</td>
<td>Session Control Protocol</td>
</tr>
<tr>
<td>MTTF</td>
<td>Mean Time To Failure</td>
<td>SCSI</td>
<td>Small Computer System Interface</td>
</tr>
<tr>
<td>MTTR</td>
<td>Mean Time To Recovery</td>
<td>SDLC</td>
<td>Software Development Life Cycle</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transmission Unit</td>
<td>SDN</td>
<td>Software Defined Network</td>
</tr>
<tr>
<td>NAC</td>
<td>Network Access Control</td>
<td>SED</td>
<td>Self-Encrypting Drive</td>
</tr>
<tr>
<td>NAS</td>
<td>Network Attached Storage</td>
<td>SFTP</td>
<td>Secure FTP</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>NFS</td>
<td>Network File System</td>
<td>SIEM</td>
<td>Security Incident Event Manager</td>
</tr>
<tr>
<td>NFV</td>
<td>Network Function Virtualization</td>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>NIC</td>
<td>Network Interface Controller</td>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>NIS</td>
<td>Network Information Service</td>
<td>SMB</td>
<td>Server Message Block</td>
</tr>
<tr>
<td>NOC</td>
<td>Network Operations Center</td>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>NPIV</td>
<td>N_Port ID Virtualization</td>
<td>SSD</td>
<td>Solid State Disk</td>
</tr>
<tr>
<td>NTFS</td>
<td>New Technology File System</td>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>NTLM</td>
<td>NT LAN Manager</td>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
<td>SSO</td>
<td>Single Sign-On</td>
</tr>
<tr>
<td>ODBC</td>
<td>Open Database Connectivity</td>
<td>TCO</td>
<td>Total Cost of Operations</td>
</tr>
<tr>
<td>OLA</td>
<td>Operational Level Agreement</td>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First</td>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>OVA</td>
<td>Open Virtual Appliance</td>
<td>TPM</td>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td>OVF</td>
<td>Open Virtualization Format</td>
<td>TTD</td>
<td>Technical Training Device</td>
</tr>
<tr>
<td>P2P</td>
<td>Physical to Physical</td>
<td>TTL</td>
<td>Time To Live</td>
</tr>
<tr>
<td>P2V</td>
<td>Physical to Virtual</td>
<td>UAT</td>
<td>User Acceptance Testing</td>
</tr>
</tbody>
</table>

CompTIA Cloud+ Certification Exam Objectives Version 2.0 (Exam Number: CV0-002)
<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP</td>
<td>Universal Datagram Protocol</td>
</tr>
<tr>
<td>UPS</td>
<td>Universal Power Supply</td>
</tr>
<tr>
<td>UTA</td>
<td>Universal Target Adapter</td>
</tr>
<tr>
<td>V2P</td>
<td>Virtual to Physical</td>
</tr>
<tr>
<td>V2V</td>
<td>Virtual to Virtual</td>
</tr>
<tr>
<td>VAT</td>
<td>Virtual Allocation Table</td>
</tr>
<tr>
<td>VCPU</td>
<td>Virtual CPU</td>
</tr>
<tr>
<td>VDI</td>
<td>Virtual Desktop Infrastructure</td>
</tr>
<tr>
<td>VHD</td>
<td>Virtual Hard Disk</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual LAN</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>VMDK</td>
<td>Virtual Machine Disk</td>
</tr>
<tr>
<td>VMFS</td>
<td>Virtual Machine File System</td>
</tr>
<tr>
<td>VNC</td>
<td>Virtual Network Computing</td>
</tr>
<tr>
<td>VNIC</td>
<td>Virtual NIC</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over IP</td>
</tr>
<tr>
<td>VPC</td>
<td>Virtual Private Cloud</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>VRAM</td>
<td>Virtual RAM</td>
</tr>
<tr>
<td>VRF</td>
<td>Virtual Routing and Forwarding</td>
</tr>
<tr>
<td>VRR</td>
<td>Vulnerability Remediation Request</td>
</tr>
<tr>
<td>VSAN</td>
<td>Virtual SAN</td>
</tr>
<tr>
<td>vSwitch</td>
<td>Virtual Switch</td>
</tr>
<tr>
<td>VTL</td>
<td>Virtual Tape Library</td>
</tr>
<tr>
<td>VXLAN</td>
<td>Virtual Extensible Local Area Network</td>
</tr>
<tr>
<td>WAF</td>
<td>Web Application Firewall</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WMI</td>
<td>Windows Management Implementation</td>
</tr>
<tr>
<td>WWNN</td>
<td>World Wide Node Name</td>
</tr>
<tr>
<td>WWPN</td>
<td>World Wide Port Name</td>
</tr>
<tr>
<td>WWUI</td>
<td>World Wide Unique Identifier</td>
</tr>
<tr>
<td>XaaS</td>
<td>Anything as a Service</td>
</tr>
<tr>
<td>ZFS</td>
<td>Z File System</td>
</tr>
</tbody>
</table>
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**
- Hyper-converged 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)

**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

**SPARE PARTS/HARDWARE**
- Keyboard, mouse, monitors
- Cat 6