CompTIA Cloud+ Certification Exam Objectives

EXAM NUMBER: CV0-001
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 CompetIA 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@compia.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:

<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>PERCENTAGE OF EXAMINATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Cloud Concepts and Models</td>
<td>12%</td>
</tr>
<tr>
<td>2.0 Virtualization</td>
<td>19%</td>
</tr>
<tr>
<td>3.0 Infrastructure</td>
<td>21%</td>
</tr>
<tr>
<td>4.0 Resource Management</td>
<td>13%</td>
</tr>
<tr>
<td>5.0 Security</td>
<td>16%</td>
</tr>
<tr>
<td>6.0 Systems Management</td>
<td>11%</td>
</tr>
<tr>
<td>7.0 Business Continuity in the Cloud</td>
<td>8%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Type I and Type II</th>
<th>Proprietary vs. open source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bare metal vs. OS dependent</td>
<td>Consumer vs. enterprise use</td>
</tr>
<tr>
<td>Performance and overhead considerations</td>
<td>Workstation vs. infrastructure</td>
</tr>
<tr>
<td>Hypervisor-specific system requirements</td>
<td></td>
</tr>
</tbody>
</table>

## 2.2 Install, configure and manage virtual machines and devices.

<table>
<thead>
<tr>
<th>Creating, importing and exporting template and virtual machines</th>
<th>Virtual NIC</th>
<th>Virtual switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install guest tools</td>
<td>Virtual network</td>
<td>VLAN</td>
</tr>
<tr>
<td>- Drives</td>
<td>IP address</td>
<td>- Assign IDs</td>
</tr>
<tr>
<td>- Management tools</td>
<td>Default gateway</td>
<td>- Bind interfaces</td>
</tr>
<tr>
<td>Snapshots and cloning</td>
<td>Netmask</td>
<td></td>
</tr>
<tr>
<td>Image backups vs. file backups</td>
<td>Bridging</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Virtual disks</th>
<th>Virtual switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Limits</td>
<td>- VLAN</td>
</tr>
<tr>
<td>- SCSI/ATA ID</td>
<td>- Interface configuration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Virtual switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Virtual NIC</td>
</tr>
<tr>
<td>- VLAN</td>
</tr>
</tbody>
</table>

## 2.3 Given a scenario, perform virtual resource migration.

<table>
<thead>
<tr>
<th>Establish requirements</th>
<th>Storage migration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance scheduling</td>
<td>Virtual vs. physical</td>
</tr>
<tr>
<td>Reasons</td>
<td>Online vs. offline migrations</td>
</tr>
<tr>
<td>- Performance issues</td>
<td>Physical to Virtual (P2V)</td>
</tr>
<tr>
<td>- Testing</td>
<td>Virtual to Virtual (V2V)</td>
</tr>
<tr>
<td>- Upgrading</td>
<td>Virtual to Physical (V2P)</td>
</tr>
<tr>
<td>- Utilization</td>
<td></td>
</tr>
</tbody>
</table>
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
3.0 Infrastructure

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

CompTIA Cloud+ Certification Exam Objectives Version 1.0 (Exam Number: CV0-001)
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
  - Changing default passwords
- User credentials
- 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
DAS | Direct Attached Storage
DAC | Discretionary Access Control
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
<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPelled Out</th>
<th>ACRONYM</th>
<th>SPelled Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS</td>
<td>Intrusion Protection system</td>
<td>RDP</td>
<td>Remote Desktop Protocol</td>
</tr>
<tr>
<td>IQN</td>
<td>Initiator Qualified Name</td>
<td>ReFS</td>
<td>Resilient File System</td>
</tr>
<tr>
<td>iSCSI</td>
<td>Internet SCSI</td>
<td>RIP</td>
<td>Routing Information Protocol</td>
</tr>
<tr>
<td>ISNS</td>
<td>Internet Storage Name Service</td>
<td>RPO</td>
<td>Recovery Point Objective</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
<td>RTO</td>
<td>Recovery Time Objectives</td>
</tr>
<tr>
<td>JBOD</td>
<td>Just a Bunch Of Disks</td>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>KVM</td>
<td>Keyboard Video Mouse</td>
<td>SAN</td>
<td>Storage Area Network</td>
</tr>
<tr>
<td>L2TP</td>
<td>Layer 2 Tunneling Protocol</td>
<td>SAS</td>
<td>Serial Attached SCSI</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
<td>SATA</td>
<td>Serial ATA</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
<td>SCP</td>
<td>Session Control Protocol</td>
</tr>
<tr>
<td>LUN</td>
<td>Logical Unit Number</td>
<td>SCSI</td>
<td>Small Computer System Interface</td>
</tr>
<tr>
<td>MAC</td>
<td>Mandatory Access Control</td>
<td>SDLC</td>
<td>Software Development Life Cycle</td>
</tr>
<tr>
<td>MAN</td>
<td>Metropolitan Area Network</td>
<td>SFTP</td>
<td>Secure FTP</td>
</tr>
<tr>
<td>MBR</td>
<td>Master Boot Record</td>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>MDF</td>
<td>Main Distribution Facility</td>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>MPIO</td>
<td>Multipath I/O</td>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multiprotocol Label Switching</td>
<td>SMB</td>
<td>Server Message Block</td>
</tr>
<tr>
<td>MSP</td>
<td>Managed Service Provider</td>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean Time Between Failure</td>
<td>SSD</td>
<td>Solid State Disk</td>
</tr>
<tr>
<td>MTTF</td>
<td>Mean Time To Failure</td>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>MTTR</td>
<td>Mean Time To Recovery</td>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transmission Unit</td>
<td>SSO</td>
<td>Single Sign-On</td>
</tr>
<tr>
<td>NAS</td>
<td>Network Attached Storage</td>
<td>TCO</td>
<td>Total Cost of Operations</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>NFS</td>
<td>Network File System</td>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>NIC</td>
<td>Network Interface Controller</td>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>NIS</td>
<td>Network Information Service</td>
<td>TPM</td>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td>NNTP</td>
<td>Network News Transport Protocol</td>
<td>TTD</td>
<td>Technical Training Device</td>
</tr>
<tr>
<td>NOC</td>
<td>Network Operations Center</td>
<td>TTL</td>
<td>Time To Live</td>
</tr>
<tr>
<td>NPIV</td>
<td>N_Port ID Virtualization</td>
<td>UAT</td>
<td>Universal Access Transceiver</td>
</tr>
<tr>
<td>NTFS</td>
<td>New Technology File System</td>
<td>UDP</td>
<td>Universal Diagram Protocol</td>
</tr>
<tr>
<td>ODBC</td>
<td>Open Database Connectivity</td>
<td>UPS</td>
<td>Universal Power Supply</td>
</tr>
<tr>
<td>OLA</td>
<td>Operational-Level Agreement</td>
<td>UTA</td>
<td>Universal Target Adapter</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
<td>V2P</td>
<td>Virtual to Physical</td>
</tr>
<tr>
<td>OSD</td>
<td>Object Storage Device</td>
<td>V2V</td>
<td>Virtual to Virtual</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First</td>
<td>VAT</td>
<td>Virtual Allocation Table</td>
</tr>
<tr>
<td>P2P</td>
<td>Physical to Physical</td>
<td>VCPU</td>
<td>Virtual CPU</td>
</tr>
<tr>
<td>P2V</td>
<td>Physical to Virtual</td>
<td>VDI</td>
<td>Virtual Desktop Infrastructure</td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as a Service</td>
<td>VHD</td>
<td>Virtual Hard Disk</td>
</tr>
<tr>
<td>PAT</td>
<td>Port Address Translation</td>
<td>VLAN</td>
<td>Virtual LAN</td>
</tr>
<tr>
<td>PBX</td>
<td>Public Branch Exchange</td>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>PIT</td>
<td>Point-In-Time (backup or snapshot)</td>
<td>VMFS</td>
<td>Virtual Machine File System</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
<td>VNC</td>
<td>Virtual Network Computing</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
<td>VNIC</td>
<td>Virtual NIC</td>
</tr>
<tr>
<td>QA</td>
<td>Quality Assurance</td>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>RAID</td>
<td>Redundant Array of Inexpensive Disks</td>
<td>VRAM</td>
<td>Virtual RAM</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role-Based Access Control</td>
<td>VSAN</td>
<td>Virtual SAN</td>
</tr>
<tr>
<td>Acronym</td>
<td>Spelled Out</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VsW</td>
<td>Virtual Switch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VTL</td>
<td>Virtual Tape Library</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WMI</td>
<td>Windows Management Implementation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WWNN</td>
<td>WorldWide Node Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WWPN</td>
<td>WorldWide Port Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WWUI</td>
<td>WorldWide Unique Identifier</td>
<td></td>
<td></td>
</tr>
<tr>
<td>XaaS</td>
<td>Anything as a Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ZFS</td>
<td>Z File System</td>
<td></td>
<td></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**
- 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

© 2015 CompTIA Properties, LLC, used under license by CompTIA Certifications, LLC. All rights reserved. All certification programs and education related to such programs are operated exclusively by CompTIA Certifications, LLC. CompTIA is a registered trademark of CompTIA Properties, LLC in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA Properties, LLC or of their respective owners. Reproduction or dissemination prohibited without written consent of CompTIA Properties, LLC. Printed in the U.S. 01815-Nov2015