INTRODUCTION
The CompTIA Cloud+ certification is an internationally recognized validation of the knowledge required of IT practitioners working in cloud computing environments.

Test Purpose: This exam will certify that the successful candidate has the knowledge and skills required to understand standard Cloud terminologies/methodologies, to implement, maintain, and deliver cloud technologies and infrastructures (e.g. server, network, storage, and virtualization technologies), and to understand aspects of IT security and use of industry best practices related to cloud implementations and the application of virtualization.

It is recommended for CompTIA Cloud+ candidates to have the following:
- CompTIA Network+ and/or CompTIA Storage+ Powered by SNIA, though CompTIA certifications are not required.
- Have at least 24-36 months of work experience in IT networking, network storage, or data center administration.
- Familiarity with any major hypervisor technologies for server virtualization, though vendor-specific certifications in virtualization are not required.

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>% 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><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

**Note: The bulleted lists below each objective are not exhaustive lists. Even though they are not included in this document, other examples of technologies, processes or tasks pertaining to each objective may also be included on the exam.**

(A list of acronyms used in these objectives appears at the end of this document.)
1.0 Cloud Concepts and Models

1.1 Compare and contrast cloud services.
- SaaS (according to NIST)
- IaaS (according to NIST)
- CaaS (according to NIST)
- PaaS (according to NIST)
- XaaS (according to NIST)
- DaaS (according to NIST)
- 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
  - Multitenancy 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 serve/just in time service
- Pay-as-you-grow
- Chargeback
- Ubiquitous access
- Metering resource pooling
- Multitenancy
- Cloud bursting
- Rapid deployment
- Automation

1.4 Explain object storage concepts.
- Object ID
2.0 Virtualization

2.1 Explain the differences between hypervisor types.
- Type I and Type II
  - Bare metal vs. OS dependant
  - Performance and overhead considerations
  - Hypervisor specific system requirements
- Proprietary vs. open source
- Consumer vs. enterprise use
  - Workstation vs. infrastructure

2.2 Install, configure, and manage virtual machines and devices.
- Creating, importing, and exporting template and virtual machines
- Install guest tools
  - Drives
  - Management tools
- Snapshots and cloning
- Image backups vs. file backups
- Virtual NIC
  - Virtual network
  - IP address
  - Default gateway
  - Netmask
  - Bridging
- Virtual disks
  - Limits
  - SCSI/ATA ID
- Virtual switches
  - VLAN
  - Interface configuration
- VLAN
  - Assign IDs
  - Bind interfaces
2.3 Given a scenario, perform virtual resource migration.

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

2.4 Explain the benefits of virtualization in a cloud environment.

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

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

- Virtual network components
  - Virtual NIC
  - Virtual HBA
  - Virtual router
- Shared memory
- Virtual CPU
- Storage Virtualization
  - Shared storage
  - Clustered storage
  - NPIV
3.0 Infrastructure

3.1 Compare and contrast various storage technologies.

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

3.2 Explain storage configuration concepts.

- Disk types
  - SSD vs. spinning
  - Interfaces types
  - Access speed
- Tiering
  - Performance levels of each tier
  - Policies
- RAID levels
  - RAID 1
- RAID 0
- RAID 1+0
- RAID 0+1
- RAID 5
- RAID 6

- File system types
  - UFS
  - EXT
  - NTFS
  - FAT
  - VMFS
  - ZFS

3.3 Execute storage provisioning.
- Creating LUNs
- Creating network shares
- Zoning and LUN masking
- Multipathing
- Implications of adding capacity to a NAS and SAN
  - Impact to operations
  - Downtime
  - Best practices

3.4 Given a scenario, implement appropriate network configurations.
- NAT
- PAT
- Subnetting/Supernetting
- VLAN and VLAN tagging
- Network port configurations
- Switching and routing in physical and virtual environments
  - Routing tables

3.5 Explain the importance of network optimization.
- WAN
- LAN
- MAN
- 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
  o Tape
  o SSD
  o USB
  o Disk

4.0 Network Management

4.1 Given a scenario, implement and use proper resource monitoring techniques.
  • Protocols
    o SNMP
    o WMI
    o IPMI
    o Syslog service
  • Alert methods
    o SMTP
    o SMS
    o SNMP
    o Web services
    o 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)
    o Hard limit
    o 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
    o Serial
    o USB
    o Parallel port mapping
4.4 Given a scenario, use appropriate tools for remote access.
  • Remote hypervisor access
  • RDP
  • SSH
  • Console port
  • HTTP

5.0 Security

5.1 Explain network security concepts, tools, and best practices.
  • ACLs
  • VPNs
  • IDS/IPS hardware/software-based firewalls
  • DMZ
  • Review / audit logs
  • Attacks
    o DDoS
    o Ping of death
    o Ping flood
5.2 Explain storage security concepts, methods, and best practices.
  • Obfuscation
  • Access Control Lists
5.3 Compare contrast different encryption technologies and methods.

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

5.4 Identify access control methods.

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

5.5 Implement guest and host hardening techniques.

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

---

6.0 Systems Management

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

- Network and IP planning/documentation
- Configuration standardization and documentation
• Change management best practices
  o Documentation
  o Configuration control
  o Asset accountability
  o Approval process
  o Back-out plan
• Configuration management
  o CMDB
  o Approval process
  o Configuration control
• Capacity management
  o Monitoring for changes
  o Trending
• Systems life cycle management
• Maintenance windows
  o 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
  o Memory ballooning
  o I/O throttling
  o CPU wait time
• Impact of configuration changes to the virtual environment
• Common issues
  o Disk failure
  o HBA failure
  o Memory failure
  o NIC failure
  o 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 offsite storage
• Replication types
  o Synchronous
  o Asynchronous
• RTO
• RPO
• MTBF
• MTTR
• Mission critical requirements

7.2 Deploy solutions to meet availability requirements.
• Fault tolerance
  o High availability
  o Local clustering /geoclustering
  o Non-high availability resources
• Multipathing
• Load balancing
## CompTIA Cloud+ Acronyms

### Introduction
The following is a list of acronyms which appear on the CompTIA Cloud+ exams. 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>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>APM</td>
<td>Application Performance Monitor</td>
</tr>
<tr>
<td>ATA</td>
<td>Advanced Technology Attachment</td>
</tr>
<tr>
<td>BCP</td>
<td>Bridge Control Protocol</td>
</tr>
<tr>
<td>BIA</td>
<td>Business Impact Analysis</td>
</tr>
<tr>
<td>BIOS</td>
<td>Basic Input/Output System</td>
</tr>
<tr>
<td>BMR</td>
<td>Bare Metal Restore</td>
</tr>
<tr>
<td>BPaaS</td>
<td>Business Process as a Service</td>
</tr>
<tr>
<td>BUN</td>
<td>Backup Network</td>
</tr>
<tr>
<td>C2C</td>
<td>Cloud to Cloud</td>
</tr>
<tr>
<td>C2D</td>
<td>Cloud to Database</td>
</tr>
<tr>
<td>CAB</td>
<td>Change Advisory Board</td>
</tr>
<tr>
<td>CAN</td>
<td>Campus Area Network</td>
</tr>
<tr>
<td>CaaS</td>
<td>Communication as a Service / Computing as a Service</td>
</tr>
<tr>
<td>CAS</td>
<td>Content Addressed Storage</td>
</tr>
<tr>
<td>CIIS</td>
<td>Client Integration Implementation Service</td>
</tr>
<tr>
<td>CMDB</td>
<td>Configuration Management Database</td>
</tr>
<tr>
<td>CNA</td>
<td>Converged Network Adapter</td>
</tr>
<tr>
<td>COLO</td>
<td>Co-Location</td>
</tr>
<tr>
<td>COOP</td>
<td>Continuity of Operations Plan</td>
</tr>
<tr>
<td>CRL</td>
<td>Certificate Revocation List</td>
</tr>
<tr>
<td>CRM</td>
<td>Customer Relationship Management</td>
</tr>
<tr>
<td>CSP</td>
<td>Content Service Provider</td>
</tr>
<tr>
<td>D2C</td>
<td>Datacenter to Cloud</td>
</tr>
<tr>
<td>DaaS</td>
<td>Data as a Service</td>
</tr>
<tr>
<td>DAC</td>
<td>Discresionary Access Control</td>
</tr>
<tr>
<td>DAS</td>
<td>Direct Attached Storage</td>
</tr>
<tr>
<td>DBaaS</td>
<td>Database as a Service</td>
</tr>
<tr>
<td>DBMS</td>
<td>Database Management Server</td>
</tr>
<tr>
<td>DCB</td>
<td>Datacenter Bridging</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Control Protocol</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Service</td>
</tr>
<tr>
<td>DRP</td>
<td>Disaster Recovery Plan</td>
</tr>
<tr>
<td>FC</td>
<td>Fibre Channel</td>
</tr>
<tr>
<td>FCoE</td>
<td>Fibre Channel over Ethernet</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>ftps</td>
<td>FTP over SSL</td>
</tr>
<tr>
<td>GPT</td>
<td>GUID Partition Table</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>HA</td>
<td>High Availability</td>
</tr>
<tr>
<td>HAV</td>
<td>Hardware Assisted Virtualization</td>
</tr>
<tr>
<td>HBA</td>
<td>Host Bus Adapter</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>IaaS</td>
<td>Infrastructure as a Service</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Management Protocol</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IFCP</td>
<td>Internet Fibre Channel Protocol</td>
</tr>
<tr>
<td>IPMI</td>
<td>Intelligent Platform Management Interface</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Protection system</td>
</tr>
<tr>
<td>IQN</td>
<td>Initiator Qualified Name</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>iSCSI</td>
<td>Internet SCSI</td>
</tr>
<tr>
<td>ISNS</td>
<td>Internet Storage Name Service</td>
</tr>
<tr>
<td>JBOD</td>
<td>Just of bunch of Disks</td>
</tr>
<tr>
<td>L2TP</td>
<td>Layer 2 Tunneling Protocol</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LUN</td>
<td>Logical Unit Number</td>
</tr>
<tr>
<td>MAC</td>
<td>Mandatory Access Control</td>
</tr>
<tr>
<td>MAN</td>
<td>Metropolitan Area Network</td>
</tr>
<tr>
<td>MBR</td>
<td>Master Boot Record</td>
</tr>
<tr>
<td>MDF</td>
<td>Main Distribution Facility</td>
</tr>
<tr>
<td>MSP</td>
<td>Managed Service Provider</td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean Time Between Failure</td>
</tr>
<tr>
<td>MTTF</td>
<td>Mean Time To Failure</td>
</tr>
<tr>
<td>MTTR</td>
<td>Mean Time To Recovery</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transmission Unit</td>
</tr>
<tr>
<td>NAS</td>
<td>Network Attached Storage</td>
</tr>
<tr>
<td>NFS</td>
<td>Network File System</td>
</tr>
<tr>
<td>NIS</td>
<td>Network Information Service</td>
</tr>
<tr>
<td>NNTP</td>
<td>Network News Transport Protocol</td>
</tr>
<tr>
<td>NOC</td>
<td>Network Operations Center</td>
</tr>
<tr>
<td>NPIV</td>
<td>N_Port ID Virtualization</td>
</tr>
<tr>
<td>OLA</td>
<td>Operational Level Agreement</td>
</tr>
<tr>
<td>OSD</td>
<td>Object Storage Device</td>
</tr>
<tr>
<td>P2P</td>
<td>Physical to Physical</td>
</tr>
<tr>
<td>P2V</td>
<td>Physical to Virtual</td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as a Service</td>
</tr>
<tr>
<td>PAT</td>
<td>Port Address Translation</td>
</tr>
<tr>
<td>PIT</td>
<td>Point-in-Time backup or snapshot</td>
</tr>
<tr>
<td>QA</td>
<td>Quality Assurance</td>
</tr>
<tr>
<td>RAID</td>
<td>Redundant Array of Inexpensive Disks</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role-based Access Control</td>
</tr>
<tr>
<td>PBX</td>
<td>Public Branch Exchange</td>
</tr>
<tr>
<td>RDP</td>
<td>Remote Desktop Protocol</td>
</tr>
<tr>
<td>RIP</td>
<td>Routing Information Protocol</td>
</tr>
<tr>
<td>RPO</td>
<td>Recovery Point Objective</td>
</tr>
<tr>
<td>RTO</td>
<td>Recovery Time Objectives</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SAN</td>
<td>Storage Area Network</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>SAS</td>
<td>Serial Attached SCSI</td>
</tr>
<tr>
<td>SATA</td>
<td>Serial ATA</td>
</tr>
<tr>
<td>SCSI</td>
<td>Small Computer System Interface</td>
</tr>
<tr>
<td>SDLC</td>
<td>Software Development Life Cycle</td>
</tr>
<tr>
<td>SFTP</td>
<td>Secure FTP</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SSD</td>
<td>Solid State Disk</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign-On</td>
</tr>
<tr>
<td>TCO</td>
<td>Total Cost of Operations</td>
</tr>
<tr>
<td>TTD</td>
<td>Technical Training Device</td>
</tr>
<tr>
<td>UAT</td>
<td>Universal Access Transceiver</td>
</tr>
<tr>
<td>UDP</td>
<td>Universal Diagram 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>VLAN</td>
<td>Virtual LAN</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>VNIC</td>
<td>Virtual NIC</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>VRAM</td>
<td>Virtual RAM</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>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WWNN</td>
<td>WorldWide Node Name</td>
</tr>
<tr>
<td>WWPN</td>
<td>WorldWide Port Name</td>
</tr>
<tr>
<td>XaaS</td>
<td>anything as a Service</td>
</tr>
</tbody>
</table>
Suggested Classroom Equipment to have for Cloud+ Certification Training

** 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
- Screw drivers
- 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