Learnsoft
ENTERPRISE TRAINING

4350 Executive Drive, Suite 100
San Diego, CA 92121
San Diego (858) 546-1400

CompTIA Cloud+

Length: 5 Days

Who Should Attend:

- Project manager, cloud computing services
- Cloud engineer
- Manager, data center SAN
- Business analyst, cloud computing

Summary: The CompTIA Cloud+ certification validates the knowledge and best practices required of IT practitioners working in cloud computing environments, who must understand and deliver cloud infrastructure. Recommended experience includes at least 24-36 months of work experience in IT networking, storage, or data center administration, and familiarity with any major hypervisor technologies for server virtualization.

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

Exam: CV0-001

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.

Recommended Skills/Knowledge

It is recommended for CompTIA Cloud+ candidates to have the following:

- CompTIA Network+ and/or CompTIA Storage+ 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.

Course Content

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
- 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
- Metadata
- Data/blob
- Extended metadata
- Policies
- Replicas
- Access control

2.0 Virtualization

2.1 Explain the differences between hypervisor types.

- Type I and Type II
- Proprietary vs. open source
- Consumer vs. enterprise use

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

- Creating, importing, and exporting template and virtual machines
- Install guest tools
- Snapshots and cloning
- Image backups vs. file backups
- Virtual NIC
- Virtual disks
- Virtual switches
- VLAN
- VSAN

2.3 Given a scenario, perform virtual resource migration.

- Establish requirements
- Maintenance scheduling
- Reasons
- Storage migration
- 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
- 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
- Shared memory
- Virtual CPU
- Storage Virtualization

3.0 Infrastructure

3.1 Compare and contrast various storage technologies.

- Network Attached Storage (NAS)
- Direct Attached Storage (DAS)
- Storage Area Network (SAN)
- Different access protocols
- Protocols and applications
- Management differences

3.2 Explain storage configuration concepts.

- Disk types
- Tiering
- RAID levels
- File system types

3.3 Execute storage provisioning.

- Creating LUNs
- Creating network shares
- Zoning and LUN masking
- Multipathing
- Implications of adding capacity to a NAS and SAN

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

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
- 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
- Common protocols
- Types of networks

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

4.0 Network Management

4.1 Given a scenario, implement and use proper resource monitoring techniques.

- Protocols
- Alert methods
- 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)
- 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

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

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 contrast different encryption technologies and methods.

- PKI
- IPSEC
- SSL/TLS
- Ciphers
- 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
- 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
- Configuration management
- Capacity management
- Systems life cycle management
- Maintenance windows

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
- Impact of configuration changes to the virtual environment
- Common issues

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
- Multpathing
- Load balancing
- Scaling

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
- RTO
- RPO
- MTBF
- MTTR
- Mission critical requirements

7.2 Deploy solutions to meet availability requirements.

- Fault tolerance
- Multipathing
- Load balancing