Certification Exam Objectives: SK0-004

INTRODUCTION

The CompTIA Server+ certification is an international vendor neutral credential. The CompTIA Server+ exam is a validation of "foundation" level server skills and knowledge, and is used by organizations and IT professionals around the globe.

The skills and knowledge measured by this examination are derived from an industry-wide Job Task Analysis (JTA) and were validated through a global survey in Q3, 2014. The results of the survey were used to validate the content of the subject areas (domains) and exam objectives, as well as the overall domain weightings, ensuring the importance of one domain relative to another.

The CompTIA Server+ certification is targeted towards individuals with 18-24 months of IT experience. Although not a prerequisite, it is highly recommended that candidates pursuing the CompTIA Server+ certification hold a CompTIA A+ certification or have equivalent experience.

This exam will certify that the successful candidate has the knowledge and skills required to build, maintain, troubleshoot, secure and support server hardware and software technologies, including virtualization. The successful candidate will be able to identify environmental issues, understand and comply with disaster recovery and general security procedures, be familiar with industry terminology and concepts, and understand server roles and their interaction in a dynamic computing environment.

The table below lists the domains measured by this examination and the appropriate extent to which they are represented.

Domain	% of Examination
1.0 Server Architecture	12%
2.0 Server Administration	24%
3.0 Storage	12%
4.0 Security	13%
5.0 Networking	10%
6.0 Disaster Recovery	9%
7.0 Troubleshooting	20%
Total	**100%**

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 webpage:
http://certification.comptia.org/Training/testingcenters/policies.aspx

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
(http://certification.comptia.org/Training/testingcenters/policies/agreement.aspx) at the time of exam delivery.

If a candidate has a question as to whether study materials are considered unauthorized (aka brain dumps), he/she should perform a search using CertGuard's
engine, found here:
http://www.certguard.com/search.asp

Or verify against this list:
http://certification.comptia.org/Training/testingcenters/policies/unauthorized.aspx

**Note: The lists of examples provided in bulleted format below each objective 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.

(A list of acronyms used in these Objectives appears at the end of this document.)

1.0 Server Architecture

1.1 Explain the purpose and function of server form factors

- Rack mount
  - Dimensions
    - 1U, 2U, 4U
  - Cable management arms
  - Rail kits
- Tower
- Blade technology
  - Blade enclosure
    - Backplane / Midplane
    - Power supply sockets
    - Network modules / switches
    - Management modules
  - Blade server

1.2 Given a scenario, install, configure and maintain server components

- CPU
  - Multiprocessor vs. multicore
  - Socket type
  - Cache levels: L1, L2, L3
  - Speeds
    - Core
    - Bus
    - Multiplier
  - CPU stepping
  - Architecture
    - x86
    - x64
    - ARM
- RAM
  - ECC vs. non-ECC
  - DDR2, DDR3
  - Number of pins
  - Static vs. dynamic
  - Module placement
  - CAS latency
  - Timing
  - Memory pairing
- Bus types, bus channels and expansion slots
  - Height differences and bit rate differences
  - PCI
  - PCIe
  - PCI-X
- NICs
- Hard drives
- Riser cards
- RAID controllers
- BIOS/UEFI
  - CMOS battery
- Firmware
- USB interface/port

- Hotswap vs. non-hotswap components

1.3 Compare and contrast power and cooling components

- Power
  - Voltage
    - 110v vs. 220v vs. -48v
    - 208v vs. 440v/460v/480v
  - Wattage
  - Consumption
  - Redundancy
  - 1-phase vs. 3-phase power
  - Plug types
    - NEMA
    - Edison
    - Twist lock
- Cooling
  - Airflow
  - Thermal dissipation
  - Baffles / shrouds
  - Fans
  - Liquid cooling

2.0 Server Administration

2.1 Install and configure server operating systems

- Determine server role/purpose
- Update firmware
- BIOS/UEFI configuration
  - Boot order
- Disk preparation
  - RAID setup
  - Partitioning
  - Formatting
  - File system type
    - Ext 2, 3, 4
    - NTFS
    - FAT32
    - ReiserFS
    - UFS
    - VMFS
    - ZFS
  - Swap
- Configure host name
- Local account setup
- Connect to network
- Join domain/directory
- Address security concerns
  - Patching
  - OS hardening
  - Compliance to company procedures/standards
- Enable services
- Install features/roles/applications/drivers
- Performance baseline
  - Server optimization
  - Swap or pagefile optimization

- Unattended/remote installations
    - Deploying images and cloning
    - Scripted installs
        - PXE boot
        - TFTP

2.2 Compare and contrast server roles and requirements for each

- Web server
- Application server
- Directory server
- Database server
- File server
- Print server
- Messaging server
- Mail server
- Routing and remote access server
- Network services server
    - DHCP
    - DNS/WINS
    - NTP

2.3 Given a scenario, use access and control methods to administer a server

- Local hardware administration
    - KVM
    - Serial
    - Virtual Administration console
- Network-based hardware administration
    - KVM over IP
    - ILO
    - iDRAC
- Network-based operating system administration
    - RDP
    - SSH
    - VNC
    - Command line / shell

2.4 Given a scenario, perform proper server maintenance techniques

- Change management
- Patch management
    - Operating System updates
    - Application updates
    - Security software updates
    - Firmware updates
    - Device drivers updates
    - Compatibility lists
        - Operating systems
        - Hardware
        - Applications
    - Testing and validation
- Outages & Service Level Agreements
    - Scheduled downtime
    - Unscheduled downtime
    - Impact analysis
    - Client notification
    - MTTR

- Performance monitoring
  - CPU utilization
  - Memory utilization
  - Network utilization
  - Disk utilization
    - Disk IOPS
    - Storage capacity
  - Comparison against performance baseline
  - Processes and services monitoring
  - Log monitoring
- Hardware maintenance
  - Check system health indicators
    - LEDs
    - Error codes
    - Beep codes
    - LCD messages
  - Replace failed components
    - Fans
    - Hard drives
    - RAM
    - Backplanes
    - Batteries
  - Preventative maintenance
    - Clearing dust
    - Check proper air flow
  - Proper shut down procedures
- Fault tolerance and high availability techniques
  - Clustering
    - Active/active
    - Active/passive
  - Load balancing
    - Round robin
    - Heartbeat

2.5 Explain the importance of asset management and documentation

- Asset management
  - Licensing
  - Labeling
  - Warranty
  - Life cycle management
    - Procurement
    - Usage
    - End of life
    - Disposal/recycling
  - Inventory
    - Make
    - Model
    - Serial number
    - Asset tag
- Documentation
  - Service manuals
  - Network diagrams
  - Architecture diagrams
  - Dataflow diagrams
  - Recovery documentation
  - Baseline documentation

    - Change management policies
    - Service Level Agreement
    - Server configuration
  - Secure storage of sensitive documentation

2.6 Explain the purpose and operation of virtualization components

- Hosts and guests
- Management interface for virtual machines
- Hypervisor
  - Type I
  - Type II
  - Hybrid
- Hardware compatibility list
  - BIOS/UEFI compatibility and support
  - CPU compatibility support
  - AMD-V / Intel VT
- Resource allocation between Guest and Host
  - CPU
  - Storage
  - Memory
  - Network connectivity
    - Direct Access (Bridging) vs. NAT
    - Virtual NICs
    - Virtual switches
  - Video

3.0 Storage

3.1 Given a scenario, install and deploy primary storage devices based on given specifications and interfaces

- Disk specifications
  - RPM
  - Dimensions/form factor
  - Capacity
  - Bus width
  - IOPS
  - Seek time and latency
  - Hotswap vs. non-hotswap components
- Interfaces
  - SAS
  - SATA
  - SCSI
  - USB
  - Fiber Channel
- Hard drive vs. SSD

3.2 Given a scenario, configure RAID using best practices

- RAID levels and performance considerations
  - 0
  - 1
  - 5
  - 6
  - 10
- Software vs. hardware RAID
  - Performance considerations

- Configuration specifications
  - Capacity
  - Bus types
  - Drive RPM
- Hotswap support and ramifications
- Hot spare vs. cold spare
- Array controller
  - Memory
  - Battery backed cache
  - Redundant controller

3.3 Summarize hardware and features of various storage technologies

- DAS
- NAS
  - iSCSI
  - FCoE
- SAN
  - Fiber Channel
  - LUN & LUN masking
  - HBAs and fabric switches
- JBOD
- Tape
  - Drive
  - Libraries
- Optical drive
- Flash, Compact Flash and USB drive

3.4 Given a scenario, calculate appropriate storage capacity and plan for future growth

- Base10 vs. Base2 disk size calculation (1000 vs. 1024)
- Disk quotas
- Compression
- Capacity planning considerations:
  - Operating system growth
    - Patches
    - Service packs
    - Log files
  - Temporary directories
  - Databases
  - Application servers
  - File servers
  - Archival

4.0 Security

4.1 Compare and contrast physical security methods and concepts

- Multifactor Authentication
  - Something you have
  - Something you know
  - Something you are
- Security concepts
  - Mantrap
  - RFID chip
  - ID card

    - Biometric
    - Keypad
    - Access list
    - Security guard
    - Security camera
    - Keys & Locks
        - Cabinet
        - Rack mount
        - Server
    - Safe

4.2 Given a scenario, apply server hardening techniques

- OS hardening
    - Stopping unneeded services / closing unneeded ports
    - Install only required software
    - Install latest operating system patches
- Application hardening
    - Install latest patches
    - Disabling unneeded services/roles/features
- Endpoint security
    - HIDS
    - Anti-malware
- Remediate security issues based on a vulnerability scan
- Hardware hardening
    - Disabling unneeded hardware and physical ports/devices
    - BIOS password
    - Disable WOL (Wake on LAN)
    - Setup boot order
    - Chassis locks / intrusion detection

4.3 Explain basic network security systems and protocols

- Firewall
    - Network-based
    - Host-based
- Port security / 802.1x / NAC
- Router access list
- NIDS
- Authentication protocols
    - LDAP
    - RADIUS
    - TACACS
    - TACACS+
- PKI
    - Private key
    - Public key
    - Certificate authority
    - SSL/TLS
- VPN
- IPSEC
- VLAN
- Security zones
    - DMZ
    - Public and private
    - Intranet and extranet

4.4 Implement logical access control methods based on company policy

- Access control lists
  - Users
  - Groups
    - Roles
  - Resources
    - File system
    - Network ACLs
    - Peripheral devices
    - Administrative rights
    - Distribution lists
- Permissions
  - Read
  - Write/Modify
  - Execute
  - Delete
  - Full control/Superuser
  - File vs. share

4.5 Implement data security methods and secure storage disposal techniques

- Storage encryption
  - File level encryption
  - Disk encryption
  - Tape encryption
- Storage media
  - Soft wipe
    - File deletion
  - Hard wipe
    - Zero out all sectors
  - Physical destruction
  - Remote wipe

4.6 Given a scenario, implement proper environmental controls and techniques

- Power concepts and best practices
  - UPS
    - Runtime vs. capacity
    - Automated graceful shutdown of attached devices
    - Periodic testing of batteries
    - Maximum load
    - Bypass procedures
    - Remote management
  - PDU
    - Connect redundant rack PDUs to separate circuits
  - Capacity planning
    - PDU ratings
    - UPS ratings
    - Total potential power draw
  - Multiple circuits
    - Connect redundant power supplies to separate PDUs
- Safety
  - ESD procedures
  - Fire suppression
  - Proper lifting techniques
  - Rack stability
  - Floor load limitations
  - Sharp edges and pinch points

- HVAC
  - Room and rack temperature and humidity
    - Monitoring and alert notifications
  - Air flow
    - Rack filler/baffle/blanking panels
  - Hot aisle and cold aisle

5.0 Networking

5.1 Given a scenario, configure servers to use IP addressing and network infrastructure services

- IPv4 vs. IPv6
- Default gateway
- CIDR notation and subnetting
- Public and private IP addressing
- Static IP assignment vs. DHCP
- DNS
  - FQDN
  - Default domain suffix / search domain
- WINS
- NetBIOS
- NAT/PAT
- MAC addresses
- Network Interface Card configuration
  - NIC teaming
  - Duplexing
    - Full
    - Half
    - Auto
  - Speeds
    - 10/100/1000 Mbps
    - 10 Gbps

5.2 Compare and contrast various ports and protocols

- TCP vs. UDP
- SNMP 161
- SMTP 25
- FTP 20/21
- SFTP 22
- SSH 22
- SCP 22
- NTP 123
- HTTP 80
- HTTPS 443
- TELNET 23
- IMAP 143
- POP3 110
- RDP 3389
- FTPS 989/990
- LDAP 389/3268
- DNS 53
- DHCP 68

5.3 Given a scenario, install cables and implement proper cable management procedures

- Copper
  - Patch cables
    - Crossover
    - Straight through
    - Rollover
  - CAT5
  - CAT5e
  - CAT6
- Fiber
  - Singlemode
  - Multimode
- Connectors
  - ST
  - LC
  - SC
  - SFP
  - RJ-45
  - RJ-11
- Cable placement and routing
  - Cable channels
  - Cable management trays
    - Vertical
    - Horizontal
- Labeling
- Bend radius
- Cable ties

6.0 Disaster Recovery

6.1 Explain the importance of disaster recovery principles

- Site types
  - Hot site
  - Cold site
  - Warm site
- Replication methods
  - Disk to disk
  - Server to server
  - Site to site
- Continuity of Operations
  - Disaster recovery plan
  - Business continuity plan
  - Business impact analysis
    - Who is affected
    - What is affected
    - Severity of impact

6.2 Given a scenario, implement appropriate backup techniques

- Methodology
  - Full/Normal
    - Copy
  - Incremental
  - Differential
  - Snapshot

    - Selective
    - Bare metal
    - Open file
    - Data vs. OS restore
- Backup media
    - Linear Access
        - Tape
    - Random Access
        - Disk
        - Removable media
        - Optical media
- Media and restore best practices
    - Labeling
    - Integrity verification
    - Test restorability
    - Tape rotation and retention
- Media storage location
    - Offsite
    - Onsite
    - Security considerations
    - Environmental considerations

7.0 Troubleshooting

7.1 Explain troubleshooting theory and methodologies

- Identify the problem and determine the scope
    - Question users/stakeholders and identify changes to the server / environment
    - Collect additional documentation / logs
    - If possible, replicate the problem as appropriate
    - If possible, perform backups before making changes
- Establish a theory of probable cause (question the obvious)
    - Determine whether there is a common element of symptom causing multiple problems
- Test the theory to determine cause
    - Once theory is confirmed, determine next steps to resolve problem
    - If theory is not confirmed, establish new theory or escalate
- Establish a plan of action to resolve the problem and notify impacted users
- Implement the solution or escalate as appropriate
    - Make one change at a time and test/confirm the change has resolved the problem
    - If the problem is not resolved, reverse the change if appropriate and implement new change
- Verify full system functionality and if applicable implement preventative measures
- Perform a root cause analysis
- Document findings, actions and outcomes throughout the process

7.2 Given a scenario, effectively troubleshoot hardware problems, selecting the appropriate tools and methods

- Common problems
    - Failed POST
    - Overheating
    - Memory failure

    - Onboard component failure
    - Processor failure
    - Incorrect boot sequence
    - Expansion card failure
    - Operating system not found
    - Drive failure
    - Power supply failure
    - I/O failure
- Causes of common problems
    - Third party components or incompatible components
    - Incompatible or incorrect BIOS
    - Cooling failure
    - Mismatched components
    - Backplane failure
- Environmental issues
    - Dust
    - Humidity
    - Temperature
    - Power surge / failure
- Hardware tools
    - Power supply tester (multimeter)
    - Hardware diagnostics
    - Compressed air
    - ESD equipment

7.3 Given a scenario, effectively troubleshoot software problems, selecting the appropriate tools and methods

- Common problems
    - User unable to logon
    - User cannot access resources
    - Memory leak
    - BSOD / stop
    - OS boot failure
    - Driver issues
    - Runaway process
    - Cannot mount drive
    - Cannot write to system log
    - Slow OS performance
    - Patch update failure
    - Service failure
    - Hangs no shut down
    - Users cannot print
- Cause of common problems
    - User Account Control (UAC/SUDO)
    - Corrupted files
    - Lack of hard drive space
    - Lack of system resources
    - Virtual memory (misconfigured, corrupt)
    - Fragmentation
    - Print server drivers/services
    - Print spooler
- Software tools
    - System logs
    - Monitoring tools (resource monitor, performance monitor)
    - Defragmentation tools
    - Disk property tools (usage, free space, volume or drive mapping)

7.4 Given a scenario, effectively diagnose network problems, selecting the appropriate tools and methods

- Common problems
  - Internet connectivity failure
  - Email failure
  - Resource unavailable
  - DHCP server mis-configured
  - Non-functional or unreachable
  - Destination host unreachable
  - Unknown host
  - Default gateway mis-configured
  - Failure of service provider
  - Cannot reach by host name/FQDN
- Causes of common problems
  - Improper IP configuration
  - VLAN configuration
  - Port security
  - Improper subnetting
  - Component failure
  - Incorrect OS route tables
  - Bad cables
  - Firewall (mis-configuration, hardware failure, software failure)
  - Mis-configured NIC, routing / switch issues
  - DNS and/or DHCP failure
  - Mis-configured hosts file
  - IPv4 vs. IPv6 misconfigurations
- Networking tools
  - ping
  - tracert / traceroute
  - ipconfig / ifconfig
  - nslookup
  - net use / mount
  - route
  - nbtstat
  - netstat

7.5 Given a scenario, effectively troubleshoot storage problems, selecting the appropriate tools and methods

- Common problems
  - Slow file access
  - OS not found
  - Data not available
  - Unsuccessful backup
  - Error lights
  - Unable to mount the device
  - Drive not available
  - Cannot access logical drive
  - Data corruption
  - Slow I/O performance
  - Restore failure
  - Cache failure
  - Multiple drive failure
- Causes of common problems
  - Media failure
  - Drive failure
  - Controller failure

    - HBA failure
    - Loose connectors
    - Cable problems
    - Mis-configuration
    - Improper termination
    - Corrupt boot sector
    - Corrupt file system table
    - Array rebuild
    - Improper disk partition
    - Bad sectors
    - Cache battery failure
    - Cache turned off
    - Insufficient space
    - Improper RAID configuration
    - Mis-matched drives
    - Backplane failure
- Storage tools
    - Partitioning tools
    - Disk management
    - RAID array management
    - Array management
    - System logs
    - Net use / mount command
    - Monitoring tools

7.6 Given a scenario, effectively diagnose security issues, selecting the appropriate tools and methods

- Common problems
    - File integrity issue
    - Privilege escalation
    - Applications will not load
    - Can't access network file/shares
    - Unable to open files
    - Excessive access
    - Excessive memory utilization
- Causes of common problems
    - Open ports
    - Active services
    - Inactive services
    - Intrusion detection configurations
    - Anti-malware configurations
    - Local/group policies
    - Firewall rules
    - Misconfigured permissions
    - Virus infection
    - Rogue processes/services
- Security tools
    - Port scanners
    - Sniffers
    - Cipher
    - Checksums
    - Telnet client
    - Anti-malware