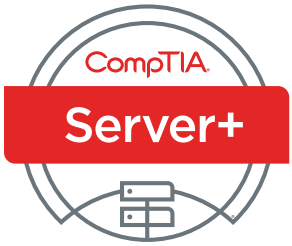

CompTIA Server+ Certification Exam Objectives

EXAM NUMBER: SK0-005

CompTIA

About the Exam

Candidates are encouraged to use this document to help prepare for the CompTIA Server+ (SK0-005) certification exam. With the end goal of proactively defending and continuously improving the security of an organization, Server+ will verify the successful candidate has the knowledge and skills required to:

- Install, configure, and manage server hardware and server operating systems
- Implement proper server hardening and security controls
- Successfully troubleshoot common server problems
- Demonstrate an understanding of key disaster recovery, high-availability, and backup concepts

This is equivalent to two years of hands-on experience working in a server environment.

These content examples are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination.

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an 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 testing exam objectives. Please know that all related exam preparation materials will still be valid.

TEST DETAILS

Required exam	SK0-005
Number of questions	90
Types of questions	Multiple choice and performance-based
Length of test	90 minutes
Recommended experience	• Two years of hands-on experience working in a server environment • CompTIA A+ certified or equivalent knowledge
Passing score	750

EXAM OBJECTIVES (DOMAINS)

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

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 Server Hardware Installation and Management	18%
2.0 Server Administration	30%
3.0 Security and Disaster Recovery	24%
4.0 Troubleshooting	28%
Total	**100%**

1.0 Server Hardware Installation and Management

1.1 Given a scenario, install physical hardware.

- **Racking**
  - Enclosure sizes
  - Unit sizes
    - 1U, 2U, 3U, etc.
  - Rack layout
    - Cooling management
    - Safety
      - Proper lifting techniques
      - Rack balancing
      - Floor load limitations
    - Power distribution unit (PDU)
    - Keyboard-video-mouse (KVM) placement
    - Rail kits
- **Power cabling**
  - Redundant power
    - Uninterruptible power supply (UPS)
    - Separate circuits
    - Separate providers
  - Power connector types
  - Cable management
- **Network cabling**
  - Redundant networking
  - Twisted pair
  - Fiber
    - SC
    - LC
    - Single mode
    - Multimode
  - Gigabit
  - 10 GigE
  - Small form factor pluggable (SFP)
  - SFP+
  - Quad small form factor pluggable (QSFP)
  - Cable management
- **Server chassis types**
  - Tower
  - Rack mount
  - Blade enclosure
- **Server components**
  - Hardware compatibility list (HCL)
  - Central processing unit (CPU)
  - Graphics processing unit (GPU)
  - Memory
  - Bus types
  - Interface types
  - Expansion cards

1.2 Given a scenario, deploy and manage storage.

- **RAID levels and types**
  - 0
  - 1
  - 5
  - 6
  - 10
  - Just a bunch of disks (JBOD)
  - Hardware vs. software
- **Capacity planning**
- **Hard drive media types**
  - Solid state drive (SSD)
    - Wear factors
      - Read intensive
      - Write intensive
  - Hard disk drive (HDD)
    - Rotations per minute (RPM)
      - 15,000
      - 10,000
      - 7,200
  - Hybrid
- **Interface types**
  - Serial attached SCSI (SAS)
  - Serial ATA (SATA)
  - Peripheral component interconnect (PCI)
  - External serial advanced technology attachment (eSATA)
  - Universal serial bus (USB)
  - Secure digital (SD)
- **Shared storage**
  - Network attached storage (NAS)
    - Network file system (NFS)
    - Common Internet file system (CIFS)
  - Storage area network (SAN)
    - Internet small computer systems interface (iSCSI)
    - Fibre Channel
    - Fibre Channel over Ethernet (FCoE)

1.3 Given a scenario, perform server hardware maintenance.

- **Out-of-band management**
  - Remote drive access
  - Remote console access
  - Remote power on/off
  - Internet protocol keyboard-video-mouse (IP KVM)
- **Local hardware administration**
  - Keyboard-video-mouse (KVM)
  - Crash cart
  - Virtual administration console
  - Serial connectivity
  - Console connections
- **Components**
  - Firmware upgrades
- **Drives**
- **Hot-swappable hardware**
  - Drives
  - Cages
  - Cards
  - Power supplies
  - Fans
- **Basic input/output system (BIOS)/Unified Extensible Firmware Interface (UEFI)**

2.0 Server Administration

2.1 Given a scenario, install server operating systems.

- **Minimum operating system (OS) requirements**
- **Hardware compatibility list (HCL)**
- **Installations**
  - Graphical user interface (GUI)
  - Core
  - Bare metal
  - Virtualized
  - Remote
  - Slip streamed/unattended
    - Scripted installations
    - Additional drivers
    - Additional applications and utilities
    - Patches
  - Media installation type
    - Network
    - Optical
    - Universal serial bus (USB)
    - Embedded
  - Imaging
    - Cloning
      - Virtual machine (VM) cloning
      - Physical clones
    - Template deployment
    - Physical to virtual (P2V)
- **Partition and volume types**
  - Global partition table (GPT) vs. master boot record (MBR)
  - Dynamic disk
  - Logical volume management (LVM)
- **File system types**
  - ext4
  - New technology file system (NTFS)
  - VMware file system (VMFS)
  - Resilient file system (ReFS)
  - Z file system (ZFS)

2.2 Given a scenario, configure servers to use network infrastructure services.

- **IP configuration**
- **Virtual local area network (VLAN)**
- **Default gateways**
- **Name resolution**
  - Domain name service (DNS)
  - Fully qualified domain name (FQDN)
  - Hosts file
- **Addressing protocols**
  - IPv4
    - Request for comments (RFC) 1918 address spaces
  - IPv6
- **Firewall**
  - Ports
- **Static vs. dynamic**
  - Dynamic host configuration protocol (DHCP)
  - Automatic private IP address (APIPA)
- **MAC addresses**

2.3 Given a scenario, configure and maintain server functions and features.

- **Server roles requirements**
  - Print
  - Database
  - File
  - Web
  - Application
  - Messaging
  - Baselining
    - Documentation
    - Performance metrics
- **Directory connectivity**
- **Storage management**
  - Formatting
  - Connectivity
  - Provisioning
  - Partitioning
  - Page/swap/scratch location and size
  - Disk quotas
  - Compression
  - Deduplication
- **Monitoring**
  - Uptime
  - Thresholds
  - Performance
    - Memory
    - Disk
      - Input output operations per second (IOPS)
      - Capacity vs. utilization
    - Network
    - Central processing unit (CPU)
  - Event logs
    - Configuration
    - Shipping
    - Alerting
    - Reporting
    - Retention
    - Rotation
- **Data migration and transfer**
  - Infiltration
  - Exfiltration
  - Disparate OS data transfer
    - Robocopy
    - File transfer
    - Fast copy
    - Secure copy protocol (SCP)
- **Administrative interfaces**
  - Console
  - Remote desktop
  - Secure shell (SSH)
  - Web interface

2.4 Explain the key concepts of high availability for servers.

- **Clustering**
  - Active-active
  - Active-passive
  - Failover
  - Failback
  - Proper patching procedures
  - Heartbeat
- **Fault tolerance**
  - Server-level redundancy vs. component redundancy
- **Redundant server network infrastructure**
  - Load balancing
    - Software vs. hardware
    - Round robin
    - Most recently used (MRU)
  - Network interface card (NIC) teaming and redundancy
    - Failover
    - Link aggregation

2.5 Summarize the purpose and operation of virtualization.

- **Host vs. guest**
- **Virtual networking**
  - Direct access (bridged)
  - Network address translation (NAT)
  - vNICs
  - Virtual switches
- **Resource allocation and provisioning**
  - CPU
  - Memory
  - Disk
  - NIC
  - Overprovisioning
  - Scalability
- **Management interfaces for virtual machines**
- **Cloud models**
  - Public
  - Private
  - Hybrid

2.6 Summarize scripting basics for server administration.

- **Script types**
  - Bash
  - Batch
  - PowerShell
  - Virtual basic script (VBS)
- **Environment variables**
- **Comment syntax**
- **Basic script constructs**
  - Loops
  - Variables
  - Conditionals
  - Comparators
- **Basic data types**
  - Integers
  - Strings
  - Arrays
- **Common server administration scripting tasks**
  - Startup
  - Shut down
  - Service
  - Login
  - Account creation
  - Bootstrap

2.7 Explain the importance of asset management and documentation.

- **Asset management**
  - Labeling
  - Warranty
  - Leased vs. owned devices
  - Life-cycle management
    - Procurement
    - Usage
    - End of life
    - Disposal/recycling
  - Inventory
    - Make
    - Model
    - Serial number
    - Asset tag
- **Documentation management**
  - Updates
  - Service manuals
  - Architecture diagrams
  - Infrastructure diagrams
  - Workflow diagrams
  - Recovery processes
  - Baselines
  - Change management
  - Server configurations
  - Company policies and procedures
    - Business impact analysis (BIA)
    - Mean time between failure (MTBF)
    - Mean time to recover (MTTR)
    - Recovery point objective (RPO)
    - Recovery time objective (RTO)
    - Service level agreement (SLA)
    - Uptime requirements
- **Document availability**
- **Secure storage of sensitive documentation**

2.8 Explain licensing concepts.

- **Models**
  - Per-instance
  - Per-concurrent user
  - Per-server
  - Per-socket
  - Per-core
  - Site-based
  - Physical vs. virtual
  - Node-locked
  - Signatures
- **Open source**
- **Subscription**
- **License vs. maintenance and support**
- **Volume licensing**
- **License count validation**
  - True up
- **Version compatibility**
  - Backward compatible
  - Forward compatible

3.0 Security and Disaster Recovery

3.1 Summarize data security concepts.

- **Encryption paradigms**
  - Data at rest
  - Data in transit
- **Retention policies**
- **Data storage**
  - Physical location storage
  - Off-site vs. on-site
- **UEFI/BIOS passwords**
- **Bootloader passwords**
- **Business impact**
  - Data value prioritization
  - Life-cycle management
  - Cost of security vs. risk and/or replacement

3.2 Summarize physical security concepts.

- **Physical access controls**
  - Bollards
  - Architectural reinforcements
    - Signal blocking
    - Reflective glass
    - Datacenter camouflage
  - Fencing
  - Security guards
  - Security cameras
  - Locks
    - Biometric
    - Radio frequency identification (RFID)
    - Card readers
  - Mantraps
  - Safes
- **Environmental controls**
  - Fire suppression
  - Heating, ventilation, and cooling (HVAC)
  - Sensors

3.3 Explain important concepts pertaining to identity and access management for server administration.

- **User accounts**
- **User groups**
- **Password policies**
  - Length
  - Lockout
  - Enforcement
- **Permissions and access controls**
  - Role-based
  - Rule-based
  - Scope based
  - Segregation of duties
  - Delegation
- **Auditing**
  - User activity
  - Logins
  - Group memberships
  - Deletions
- **Multifactor authentication (MFA)**
  - Something you know
  - Something you have
  - Something you are
- **Single sign-on (SSO)**

3.4 Explain data security risks and mitigation strategies.

- **Security risks**
  - Hardware failure
  - Malware
  - Data corruption
  - Insider threats
  - Theft
    - Data loss prevention (DLP)
    - Unwanted duplication
    - Unwanted publication
  - Unwanted access methods
    - Backdoor
    - Social engineering
  - Breaches
    - Identification
    - Disclosure
- **Mitigation strategies**
  - Data monitoring
  - Log analysis
    - Security information and event management (SIEM)
  - Two-person integrity
    - Split encryption keys tokens
    - Separation of roles
  - Regulatory constraints
    - Governmental
    - Individually privileged information
      - Personally identifiable information (PII)
      - Payment Card Industry Data Security Standard (PCI DSS)
  - Legal considerations
    - Data retention
    - Subpoenas

3.5 Given a scenario, apply server hardening methods.

- **OS hardening**
  - Disable unused services
  - Close unneeded ports
  - Install only required software
  - Apply driver updates
  - Apply OS updates
  - Firewall configuration
- **Application hardening**
  - Install latest patches
  - Disable unneeded services, roles, or features
- **Host security**
  - Antivirus
  - Anti-malware
  - Host intrusion detection system (HIDS)/Host intrusion prevention system (HIPS)
- **Hardware hardening**
  - Disable unneeded hardware
  - Disable unneeded physical ports, devices, or functions
  - Set BIOS password
  - Set boot order
- **Patching**
  - Testing
  - Deployment
  - Change management

3.6 Summarize proper server decommissioning concepts.

- **Proper removal procedures**
  - Company policies
  - Verify non-utilization
  - Documentation
    - Asset management
    - Change management
- **Media destruction**
  - Disk wiping
  - Physical
    - Degaussing
    - Shredding
    - Crushing
    - Incineration
  - Purposes for media destruction
- **Media retention requirements**
- **Cable remediation**
  - Power
  - Networking
- **Electronics recycling**
  - Internal vs. external
  - Repurposing

3.7 Explain the importance of backups and restores.

- **Backup methods**
  - Full
  - Synthetic full
  - Incremental
  - Differential
  - Archive
  - Open file
  - Snapshot
- **Backup frequency**
- **Media rotation**
- **Backup media types**
  - Tape
  - Cloud
  - Disk
  - Print
- **File-level vs. system-state backup**
- **Restore methods**
  - Overwrite
  - Side by side
  - Alternate location path
- **Backup validation**
  - Media integrity
  - Equipment
  - Regular testing intervals
- **Media inventory before restoration**

3.8 Explain the importance of disaster recovery.

- **Site types**
  - Hot site
  - Cold site
  - Warm site
  - Cloud
  - Separate geographic locations
- **Replication**
  - Constant
  - Background
  - Synchronous vs. asynchronous
  - Application consistent
  - File locking
  - Mirroring
  - Bidirectional
- **Testing**
  - Tabletops
  - Live failover
  - Simulated failover
  - Production vs. non-production

4.0 Troubleshooting

4.1 Explain the troubleshooting theory and methodology.

- **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.
  - Escalate, if necessary.
- **Establish a theory of probable cause (question the obvious).**
  - Determine whether there is a common element or symptom causing multiple problems.
- **Test the theory to determine the cause.**
  - Once the theory is confirmed, determine the next steps to resolve the problem.
  - If the theory is not confirmed, establish a new theory.
- **Establish a plan of action to resolve the problem.**
  - Notify impacted users.
- **Implement the solution or escalate.**
  - 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 a new change.
- **Verify full system functionality and, if applicable, implement preventive measures.**
- **Perform a root cause analysis.**
- **Document findings, actions, and outcomes throughout the process.**

4.2 Given a scenario, troubleshoot common hardware failures.

- **Common problems**
  - Predictive failures
  - Memory errors and failures
    - System crash
      - Blue screen
      - Purple screen
      - Memory dump
    - Utilization
    - Power-on self-test (POST) errors
    - Random lockups
    - Kernel panic
  - Complementary metal-oxide-semiconductor (CMOS) battery failure
  - System lockups
  - Random crashes
  - Fault and device indication
    - Visual indicators
      - Light-emitting diode (LED)
      - Liquid crystal display (LCD) panel readouts
        - Auditory or olfactory cues
        - POST codes
  - Misallocated virtual resources
- **Causes of common problems**
  - Technical
    - Power supply fault
    - Malfunctioning fans
    - Improperly seated heat sink
    - Improperly seated cards
    - Incompatibility of components
    - Cooling failures
    - Backplane failure
    - Firmware incompatibility
    - CPU or GPU overheating
  - Environmental
    - Dust
    - Humidity
    - Temperature
- **Tools and techniques**
  - Event logs
  - Firmware upgrades or downgrades
  - Hardware diagnostics
  - Compressed air
  - Electrostatic discharge (ESD) equipment
  - Reseating or replacing components and/or cables

4.3 Given a scenario, troubleshoot storage problems.

- **Common problems**
  - Boot errors
  - Sector block errors
  - Cache battery failure
  - Read/write errors
  - Failed drives
  - Page/swap/scratch file or partition
  - Partition errors
  - Slow file access
  - OS not found
  - Unsuccessful backup
  - 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**
  - Disk space utilization
    - Insufficient disk space
  - Misconfigured RAID
  - Media failure
  - Drive failure
  - Controller failure
  - Hot bus adapter (HBA) failure
  - Loose connectors
  - Cable problems
  - Misconfiguration
  - Corrupt boot sector
  - Corrupt filesystem table
  - Array rebuild
  - Improper disk partition
  - Bad sectors
  - Cache battery failure
  - Cache turned off
  - Insufficient space
  - Improper RAID configuration
  - Mismatched drives
  - Backplane failure
- **Tools and techniques**
  - Partitioning tools
  - Disk management
  - RAID and array management
  - System logs
  - Disk mounting commands
    - net use
    - mount
  - Monitoring tools
  - Visual inspections
  - Auditory inspections

4.4 Given a scenario, troubleshoot common OS and software problems.

- **Common problems**
  - Unable to log on
  - Unable to access resources
  - Unable to access files
  - System file corruption
  - End of life/end of support
  - Slow performance
  - Cannot write to system logs
  - Service failures
  - System or application hanging
  - Freezing
  - Patch update failure
- **Causes of common problems**
  - Incompatible drivers/modules
  - Improperly applied patches
  - Unstable drivers or software
  - Server not joined to domain
  - Clock skew
  - Memory leaks
  - Buffer overrun
  - Incompatibility
    - Insecure dependencies
    - Version management
    - Architecture
  - Update failures
  - Missing updates
  - Missing dependencies
  - Downstream failures due to updates
  - Inappropriate application-level permissions
  - Improper CPU affinity and priority
- **OS and software tools and techniques**
  - Patching
    - Upgrades
    - Downgrades
  - Package management
  - Recovery
    - Boot options
      - Safe mode
      - Single user mode
    - Reload OS
    - Snapshots
  - Proper privilege escalations
    - runas/Run As
    - sudo
    - su
  - Scheduled reboots
  - Software firewalls
    - Adding or removing ports
    - Zones
  - Clocks
    - Network time protocol (NTP)
    - System time
  - Services and processes
    - Starting
    - Stopping
    - Status identification
    - Dependencies
  - Configuration management
    - System center configuration manager (SCCM)
    - Puppet/Chef/Ansible
    - Group Policy Object (GPO)
  - Hardware compatibility list (HCL)

4.5 Given a scenario, troubleshoot network connectivity issues.

- **Common problems**
  - Lack of Internet connectivity
  - Resource unavailable
  - Receiving incorrect DHCP information
  - Non-functional or unreachable
  - Destination host unreachable
  - Unknown host
  - Unable to reach remote subnets
  - Failure of service provider
  - Cannot reach server by hostname/ fully qualified domain name (FQDN)
- **Causes of common problems**
  - Improper IP configuration
  - IPv4 vs. IPv6 misconfigurations
  - Improper VLAN configuration
  - Network port security
  - Component failure
  - Incorrect OS route tables
  - Bad cables
  - Firewall (misconfiguration, hardware failure, software failure)
  - Misconfigured NIC
  - DNS and/or DHCP failure
  - DHCP server misconfigured
  - Misconfigured hosts file
- **Tools and techniques**
  - Check link lights
  - Confirm power supply
  - Verify cable integrity
  - Check appropriate cable selection
  - Commands
    - ipconfig
    - ip addr
    - ping
    - tracert
    - traceroute
    - nslookup
    - netstat
    - dig
    - telnet
    - nc
    - nbtstat
    - route

4.6 Given a scenario, troubleshoot security problems.

- **Common concerns**
  - File integrity
  - Improper privilege escalation
    - Excessive access
  - Applications will not load
  - Cannot access network fileshares
  - Unable to open files
- **Causes of common problems**
  - Open ports
  - Services
    - Active
    - Inactive
    - Orphan/zombie
  - Intrusion detection configurations
  - Anti-malware configurations
  - Improperly configured local/group policies
  - Improperly configured firewall rules
  - Misconfigured permissions
  - Virus infection
  - Malware
  - Rogue processes/services
  - Data loss prevention (DLP)
- **Security tools**
  - Port scanners
  - Sniffers
  - Telnet clients
  - Anti-malware
  - Antivirus
  - File integrity
    - Checksums
    - Monitoring
    - Detection
    - Enforcement
  - User access controls
    - SELinux
    - User account control (UAC)

CompTIA Server+ (SK0-005) Acronym List

The following is a list of acronyms that appear on the CompTIA Server+ 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
AD	Active Directory
APIPA	Automatic Private IP Address
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BIOS	Basic Input/Output System
BSOD	Blue Screen of Death
CIDR	Classless Inter-Domain Routing
CIFS	Common Internet File System
CIMC	Cisco Integrated Management Controller
CLI	Command Line Interface
CMOS	Complementary Metal-Oxide-Semiconductor
COOP	Continuity of Operations
CPU	Central Processing Unit
CRU	Customer Replaceable Unit
DAS	Direct Attached Storage
DC	Domain Controller
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DLT	Digital Linear Tape
DMZ	Demilitarized Zone
DNS	Domain Name Service
DR	Disaster Recovery
ECC	Error Checking and Correction
EFS	Encrypting File System
eSATA	External Serial Advanced Technology Attachment
ESD	Electrostatic Discharge
FAT	File Allocation Table
FCoE	Fibre Channel over Ethernet
FQDN	Fully Qualified Domain Name
FRU	Field Replaceable Unit
FTP	File Transfer Protocol
FTPS	File Transfer Protocol over SSL
GFS	Grandfather Father Son
GPO	Group Policy Object
GPT	GUID Partition Table

ACRONYM	SPELLED OUT
GPU	Graphics Processing Unit
GUI	Graphical User Interface
HBA	Host Bus Adapter
HCL	Hardware Compatibility List
HID	Human Interface Device
HIDS	Host Intrusion Detection System
HIPS	Host Intrusion Prevention System
HTTP	Hyper Text Transport Protocol
HTTPS	Secure Hyper Text Transport Protocol
HVAC	Heating Ventilation and Air Conditioning
IDF	Intermediate Distribution Frame
iDRAC	Integrated Dell Remote Access Control
IDS	Intrusion Detection System
IIS	Internet Information Services
iLO	Integrated Lights Out
IMAP4	Internet Mail Access Protocol
Intel-VT	Intel Virtualization Technology
IOPS	Input Output Operations per Second
IP	Internet Protocol
IP KVM	Internet Protocol Keyboard-Video-Mouse
IPMI	Intelligent Platform Management Interface
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
IPv6	Internet Protocol version 6
iSCSI	Internetworking Small Computer System Interface
ISO	International Organization for Standardization
JBOD	Just a Bunch of Disks
KVM	Keyboard-Video-Mouse
LAN	Local Area Network
LC	Lucent Connector/Little Connector
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
LTO	Linear Tape-Open
LUN	Logical Unit Number
LVM	Logical Volume Management
MAC	Media Access Control

ACRONYM	SPELLED OUT
MBR	Master Boot Record
MDF	Main Distribution Frame
MFA	Multifactor Authentication
MIB	Management Information Base
MMC	Microsoft Management Console
MRU	Most Recently Used
MTBF	Mean Time Between Failure
MTTR	Mean Time to Recover
NAC	Network Access Control
NAS	Network Attached Storage
NAT	Network Address Translation
NetBIOS	Network Basic Input Output System
NFS	Network File System
NIC	Network Interface Card
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
NLB	Network Load Balancing
NOS	Network Operating System
NTFS	New Technology File System
NTP	Network Time Protocol
OEM	Original Equipment Manufacturer
OS	Operating System
OTP	One-Time Password
OU	Organizational Units
P2V	Physical to Virtual
PAT	Port Address Translation
PCI	Peripheral Component Interconnect
PCI DSS	Payment Card Industry Data Security Standard
PCIe	Peripheral Component Interconnect Express
PCI-X	Peripheral Component Interconnect Extended
PDU	Power Distribution Unit
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
POST	Power on Self-Test
PSU	Power Supply Unit
PXE	Preboot Execution Environment
QSFP	Quad-Small Form Factor Pluggable
RADIUS	Remote Authentication Dial-in User Service
RAID	Redundant Array of Inexpensive/Integrated Disks/Drives
RAM	Random Access Memory
RAS	Remote Access Server
RDP	Remote Desktop Protocol
ReFS	Resilient File System
RFC	Request for Comments
RFID	Radio Frequency Identification
RIS	Remote Installation Service
RJ45	Registered Jack 45
RPM	Rotations per Minute
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAN	Storage Area Network
SAS	Serial Attached SCSI
SATA	Serial ATA
SC	Standard Connector
SCCM	System Center Configuration Management
SCP	Secure Copy Protocol
SCSI	Small Computer System Interface
SD	Secure Digital
SELinux	Security Enhanced Linux
SFP	Small Form Factor Pluggable
SFTP	Secure File Transfer Protocol
SLA	Service Level Agreement
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSD	Solid State Drive
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On
ST	Straight Tip
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UAC	User Account Control
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UID	Unit Identification
UPS	Uninterruptible Power Supply
URL	Universal/Uniform Resource Locator
USB	Universal Serial Bus
UUID	Universal Unique Identifier
VBS	Visual Basic Script
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMFS	VMWare File System
VNC	Virtual Network Computing
vNIC	Virtual Network Interface Card
VoIP	Voice over IP
VPN	Virtual Private Network
VSS	Volume Shadow Service
VT	Virtualization Technology
WDS	Windows Deployment Services
WINS	Windows Internet Naming Service
WMI	Windows Management Instrumentation
WOL	Wake on LAN
WSUS	Windows Software Update Services
WWNN	World Wide Node Name
WWPN	World Wide Port Name
XD	Execute Disable
ZFS	Z File System

Server+ Proposed Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the Server+ exam. This list may also be helpful for training companies that wish to create a lab component for their training offering. The bulleted lists below each topic are samples and are not exhaustive.

HARDWARE

- Computer capable of virtualization
- Cables
- USB flash drive
- KVM*
- Rack*
- UPS*
- Switch*
- Storage device*

*Ideal, but not necessary for lab setup

SOFTWARE

- Server operating system
- Virtualization software
- Antivirus/anti-malware