CompTIA Server+ Certification Exam Objectives

EXAM NUMBER: SK0-006 V6

CompTIA Server+ SK0-006 V6 Certification Exam
Draft Objectives Document Version 1.1

CompTIA

About the Exam

The CompTIA Server+ SK0-006 V6 certification exam will certify that the successful candidate has the knowledge and skills required to:

- Plan, deploy, configure, and administer server hardware and server operating systems (OSs).
- Manage physical and virtual server deployments throughout the life cycle in data center environments.
- Implement proper server hardening and security controls.
- Successfully monitor and troubleshoot common server issues.
- Implement business continuity (BC)/disaster recovery (DR) procedures and related technologies.
- Use AI responsibly in conjunction with server management workflows.
- Use security and compliance best practices in the server environment.

This is equivalent to 24 months of experience as a systems engineer or server engineer working in a server environment.

These content examples are meant to clarify the exam 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 (a.k.a. "brain dumps"), they 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 existing exam objectives. Please know that all related exam preparation materials will still be valid.

TEST DETAILS

Required exam	Server+ SK0-006 V6
Number of questions	TBD
Types of questions	Multiple-choice and performance-based
Length of test	TBD
Recommended experience	Systems or server engineer with 24 months of experience; A+ or equivalent knowledge; Network+
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.

DOMAIN		PERCENTAGE OF EXAMINATION
1.0	Planning and Deployment	TBD
2.0	Configuration and Administration	TBD
3.0	Security and Compliance	TBD
4.0	Data Center Operations	TBD
5.0	Performance Management and Troubleshooting	TBD
Total		**100%**

TROUBLESHOOTING METHODOLOGY KNOWLEDGE

During the job task analysis workshop for the Server+ SK0-006 V6 certification exam, subject matter experts deemed the troubleshooting methodology an effective best practice that new job incumbents should be aware of and leverage as they engage in troubleshooting new issues on the job. However, while this methodology is practical, the decision was made not to include it in the exam. While the methodology itself will not be tested, there remains an emphasis on troubleshooting within the job role context. Therefore, the troubleshooting methodology section appears here as part of this "competency standard" but does not constitute a formal objective or part of the Server+ certification exam. Training institutions that prepare individuals with very little technical knowledge and experience are encouraged to leverage this methodology, especially when such individuals might be applying for their first IT job.

The troubleshooting methodology includes the following steps:

- Identify the problem.
- Establish a theory of probable cause (question the obvious).
    - Research knowledge base/internet, if applicable.
- Test the theory to determine the cause.
- Establish a plan of action to resolve the problem and implement the solution.
- Verify full system functionality and, if applicable, implement preventive measures.
- Document findings/lessons learned, actions, and outcomes.

1.0 Planning and Deployment

1.1 Given a scenario, deploy physical hardware.

- Hardware compatibility list (HCL)
  - Central processing unit (CPU)
  - Random-access memory (RAM)
    - Registered Dual In-line Memory Module (RDIMM)
    - Unbuffered Dual In-line Memory Module (UDIMM)
    - Error-correcting code (ECC) vs. Non-ECC
    - Single-rank vs. Dual-rank
  - Graphics processing unit (GPU)
- Form factors
  - Backplane
  - Server chassis
    - Tower
    - Rack
    - Blade
- Storage
  - Capacity planning
  - Active-passive
  - Host bus adapter (HBA)
  - Internet Small Computer System Interface (iSCSI)
  - Fibre Channel
  - Storage area network (SAN)
  - Media types
    - Non-volatile Memory Express (NVMe)
    - Solid-state drive (SSD)
    - Hard disk drive (HDD)
- Redundancy
  - Best practices
    - Physical
    - Logical
- Networking requirements
- Cabling
- Out-of-band management
- Unified Extensible Firmware Interface (UEFI) vs. Basic Input/Output System (BIOS)
- Power requirements
- Equipment placement
  - Unit sizes
  - Rack sizes

1.2 Compare and contrast concepts related to scaling infrastructure.

- Hyperconverged infrastructure
- Edge computing
- Software-defined infrastructure/infrastructure as code (IaC)
- Virtualization
  - Hypervisors
    - Type 1
    - Type 2
  - Containerization
- Configuration management
- Cloud models
  - Hybrid
  - Public
  - Private
  - Service models
    - Software as a service (SaaS)
    - Infrastructure as a service (IaaS)
    - Platform as a service (PaaS)

1.3 Given a scenario, install server operating systems (OSs).

- Minimum OS hardware requirements
- Secure Boot
- Installation media
  - Universal Serial Bus (USB)
  - Digital versatile disc (DVD)
  - Secure Digital (SD) card
  - Live media

        - International Organization for Standardization (ISO) image file
    - Installation types
        - Attended vs. unattended
            - Answer file
        - Clean install
        - Automated imaging
        - In-place upgrade
        - Template-based deployment
    - Version types
        - Major
        - Minor
    - Installation methods
        - Command-line
        - Graphical user interface (GUI)-based
        - Core
        - Bare-metal
        - Networking methods
            - Preboot Execution Environment (PXE)
            - Zero-touch
            - Out-of-band
    - Filesystem types
        - ext4
        - New Technology File System (NTFS)
        - Virtual Machine File System (VMFS)
        - Resilient File System (ReFS)
        - Z file system (ZFS)
    - Partition and volume types
        - GUID [globally unique identifier] Partition Table (GPT) vs. master boot record (MBR)
        - Dynamic disk vs. basic disk
        - Logical volume management (LVM)
        - Block size

2.0 Configuration and Administration

2.1 Given a scenario, analyze requirements to configure servers.

- Configure filesystems
  - ext4
  - NTFS
  - VMFS
  - ReFS
  - ZFS
- Configure the appropriate partition and volume types
  - GPT vs. MBR
  - Dynamic disk vs. basic disk
  - LVM
- Implement the appropriate block size
- Configure network services
  - IP configuration
  - Virtual local area network (VLAN)
  - Default gateways
  - Name resolution
    - Domain Name System (DNS)
    - Fully qualified domain name (FQDN)
    - Hosts file
  - Addressing protocols
    - IPv4
    - IPv6
  - Firewall
    - Ports
  - Static vs. dynamic
    - Dynamic Host Configuration Protocol (DHCP)
    - Automatic Private IP Addressing (APIPA)
  - Media access control (MAC) addresses
- Configure components
  - Central processing unit (CPU)
  - Memory

2.2 Given a scenario, configure and maintain common services.

- Server roles
  - DHCP
  - DNS
  - Web
  - Database
  - File
  - Print
  - Message
  - Directory services
  - Remote desktop host services/Terminal Services
  - Network Policy Server (NPS)
  - Remote access server (RAS)
- Cloud service integration
  - Hybrid identity
    - Directory sync
    - Federation
  - Virtual private network (VPN) connectivity
  - Workload placement
  - Hybrid networking
- Administrative interfaces
  - Console
  - Secure Shell (SSH)
  - Web interface
  - Remote Desktop Protocol (RDP)
- Command-line tools
  - yum
  - dnf
  - apt
  - brew
  - PowerShell
- Terminal

2.3 Given a scenario, apply virtualization to a workload.

- Migration strategies
  - Physical to virtual (P2V)
  - Virtual to virtual (V2V)
- Virtual networking
  - Direct access
  - Network address translation (NAT)
  - Bridging
  - Virtual network interface card (vNIC)
  - Virtual switches
- Containers
  - Use cases
  - Life cycle
- Rightsizing and overprovisioning
- Hypervisor configuration
- Resource allocation and management
- Desired State Configuration (DSC)
- Device passthrough
- Dynamic vs. static memory

2.4 Given a scenario, implement high availability in a server environment.

- Clustering
  - Active-active
  - Active-passive
  - Heartbeat
- Load balancing
  - Round-robin method
  - Most Recently Used (MRU) method
  - Software vs. hardware implementations
- Redundancy and fault tolerance
  - Network interface card (NIC) teaming
  - Link aggregation
  - Hybrid failover
  - Cross-site
  - Hot spares
- Network paths
- Redundant array of independent disks (RAID)
  - 0
  - 1
  - 5
  - 6
  - 10
  - Hardware vs. software
- Hot-swappable components
- Elasticity
  - Vertical
  - Horizontal
  - Scale in
  - Scale out

2.5 Explain concepts related to scripting, automation, and orchestration.

- Scripting languages
  - Shell
    - Bash
    - csh
    - ksh
    - zsh
    - fish
    - PowerShell
  - Batch
  - Python
  - JavaScript
  - Visual Basic Script (VBS)
- Automation tools
  - Task Scheduler
  - cron
  - Daemons/services
- Orchestration
  - Ansible
  - Puppet
  - Chef
- Best practices
  - Sandbox environment
  - Code syntax
  - Code documentation
  - Error handling
  - Code review
- Versioning

2.6 Given a scenario, use AI to improve server management workflows.

- Use cases
  - Issue diagnosis
  - Research
  - Automation
  - Scripts and templates
    - Code assistance
  - Tool integration
  - Forecasting and predicting
  - Best practice configurations
  - Data analysis
  - Professional development
  - Communication
- Ethics
- Security
  - Permissions
  - Internal
  - External
  - Data classification
  - Enforcement
  - Liabilities

3.0 Security and Compliance

3.1 Explain common data security concepts.

- Data life cycle
  - Identification
  - Classification
  - Retention
  - Disposal
- Encryption
  - Post-quantum cryptography (PQC)
  - Data at rest
  - Data in transit
- Certificates
  - Secure Sockets Layer (SSL)
  - Transport Layer Security (TLS)
  - Root
  - Trusted
  - Certificate authority (CA)
  - Intermediate
- Control types
  - Physical
  - Network
  - Logical
    - Access control list (ACL)
- Testing types
  - Penetration testing
  - Vulnerability scan

3.2 Summarize concepts related to policies, procedures, and compliance.

- DR
  - Hot site
  - Warm site
  - Cold site
  - Cloud
  - Geographic location
  - Testing
    - Tabletop
    - Live failover
    - Simulated failover
    - Production vs. non-production
- BC
- Data handling
  - Privacy concerns
    - Personally identifiable information (PII)
- Network diagrams
- Security frameworks
  - National Institute of Standards and Technology (NIST)
  - Open Security Content Automation Protocol (OpenSCAP)
  - Center for Internet Security (CIS)
  - Security Technical Implementation Guide (STIG)
  - ISO
- Policies and procedures
  - Playbooks and runbooks
  - Life cycle
  - DR policy
  - BC policy
    - Recovery time objective (RTO)
    - Recovery point objective (RPO)
    - Mean time to recover (MTTR)
    - Mean time between failures (MTBF)
    - Service-level agreement (SLA)
  - Business impact analysis (BIA)
  - Change and configuration management
  - Audit
    - User activity
    - Logins
    - Group memberships
    - Deletion
    - Change
    - License
- Asset management
  - License life cycle
    - License vs. maintenance
  - Hardware life cycle
    - Disposal methods
  - Software life cycle
- Baselines
  - Hardware
  - OS
  - Application
  - Services
- Risk management
  - Identification
  - Risk response/handling approaches
    - Transference
    - Avoidance
    - Acceptance
    - Mitigation

3.3 Given a scenario, implement appropriate backup, data retention, and recovery strategies.

- Immutable backups
- Backup validation and recovery testing
  - Integrity
  - Equipment
  - Regular testing interval
- Air-gapped backup strategies
- Backup types
  - Incremental
  - Full
  - Differential
  - Synthetic full
  - Snapshot
  - Block-level
  - Image-level
- 3-2-1 rule
- Backup media and locations
  - Network-attached storage (NAS)
  - SAN
  - Direct-attached storage (DAS)
  - Tape
  - Cloud storage
  - Off-site
- Replication
  - Constant
  - Background
  - Synchronous vs. asynchronous
  - Application consistency
  - File loading
  - Mirroring
  - Bidirectional
- Compression
- Deduplication

3.4 Given a scenario, troubleshoot basic identity and access management (IAM) issues.

- Zero Trust–related issues
  - Connectivity
  - Permissions/access rights
  - Role-based access controls
  - Misconfigured devices
  - Unpatched devices
  - Unapproved location
  - Insecure network
- Authentication-related issues
  - Untrusted device
  - Incorrect one-time password (OTP)
  - Forgotten password
  - Time synchronization
  - Unprovisioned access
  - Misconfigured and/or unsupported protocol
- Network security issues
  - Mismatched VLAN
  - Router misconfiguration
  - Certificate expiration

3.5 Given a scenario, implement server hardening.

- Mitigation strategies
  - Zero-day work-around
  - Out-of-band updates
  - Segmentation
  - Quarantine or isolation
- Hardening techniques
  - Disable unneeded hardware
  - Disable ports and services
  - Update credentials for default accounts
  - Configure BIOS password
  - Encrypt drives
  - Endpoint security
  - Physical controls
    - Lock cages
    - Chassis lock
    - Server room access
    - Cable locks
  - Logical controls
    - Least privilege
    - Remote access control
  - Network controls
    - Firewalls
    - ACL
    - Segmentation
    - Data loss prevention (DLP)

3.6 Given a scenario, apply patch management best practices.

- Scheduling
- Communication
- Testing
  - Implementation
  - Rollback
- Classification
- Delivery
- Sourcing
- Validation
- Software bill of materials (SBOM)
- Security hot fix
- Documentation
- Patch types
  - System
  - Driver
  - Firmware
  - Application
- Use cases
  - Vulnerabilities
  - Updates
  - Enhancements
  - Bug fixes
  - Compatibility

4.0 Data Center Operations

4.1 Explain the importance of environmental considerations.

- Heating, ventilation, and air conditioning (HVAC)
  - Hot aisle
  - Cold aisle
- Blanking panels
- Fire suppression regulations
- Geographical location
- Monitoring
  - Humidity
  - Temperature
  - Dust
- Regulatory compliance
- Liquid cooling
  - Passive
  - Active
- Green IT initiatives
  - Power savings
- Sustainability

4.2 Explain safety and health considerations.

- Human safety
  - Fire suppression
    - Electrical
    - Chemical
  - Ergonomics
  - Team lifting
  - Rack balancing
  - Floor load limitations
  - Personal protective equipment (PPE)
  - Audio and visual alerting
    - Weather
    - Emergency
  - Emergency exit plan
    - Rally point
  - Contact list
  - Equipment placement considerations
  - Ladder racks
  - Fail-open
  - Safety data sheets (SDSs)
  - Work area considerations
    - Trash
    - Cardboard
    - Packing material
    - Battery disposal
    - Chemical disposal
- Equipment safety
  - Extinguishers
  - Electrostatic discharge (ESD)
  - Liquid restrictions
  - Maintenance window
    - Monthly

4.3 Explain the importance of power considerations according to best practices.

- Limitations for power
- Uninterruptable power supply (UPS)
  - Line interactive
  - Double conversion
  - Standby
- Voltages
  - 120 volts alternating current (VAC)
  - 240 VAC
  - -48 volts direct current (VDC)
  - High-voltage direct current (DC)
- Power distribution unit (PDU)
- Plug types
- Power disruptions
  - Power failure
  - Under-voltage event
  - Spikes
- Generators
- Redundancy
  - Rack-level
  - Center-level

4.4 Given a scenario, apply the appropriate connectivity solutions.

- Physical connections
  - Storage connectors
    - Serial Attached SCSI [Small Computer System Interface] (SAS)
    - Mini-SAS
    - Slim-SAS
    - Fibre Channel over Ethernet (FCoE)
    - NVMe over Fibre Channel (FC-NVMe)
    - InfiniBand
  - Fiber
    - Modes
      - Single
      - Multi
    - Connectors
      - Lucent connector (LC)
      - Standard connector (SC)
      - Multifiber push on (MPO)
    - Transceivers
      - Small Form-factor Pluggable (SFP)
      - Quad Small Form-factor Pluggable (QSFP)
      - Octal Small Form-factor Pluggable (OSFP)
  - Ethernet
    - Cat 6
    - Cat 7
    - 10GbE
- Failover
- Demarcation
- Drive interfaces
  - Serial Advanced Technology Attachment (SATA)
  - SAS
  - U.2
  - U.3
- Out-of-band management
  - Remote console
  - Shell
  - Keyboard-Video-Mouse (KVM)
  - Serial
- Cable management
- Wide area network (WAN)
  - Satellite
  - Cellular
  - Coaxial
  - Fiber
  - Digital subscriber line (DSL)

4.5 Explain the importance of security and access solutions.

- Logical controls
  - IAM
  - Geofencing
- Physical controls
  - Biometrics
  - Tokens
  - Bollards
  - Security guards
  - Cameras
  - Fences
  - Access control vestibule
  - Keys
  - Badging
  - Visitor management
- Architectural reinforcement
  - Faraday cage
  - Camouflage

5.0 Performance Management and Troubleshooting

5.1 Given a scenario, use observability strategies to manage servers.

- Logs
  - System
  - Security
  - Application
  - Centralized logging
- Alerts
  - Pager
  - Internal
  - External
  - Short Message Service (SMS)
  - Email
  - Phone
- Baseline
- Metrics
  - Heavy load
  - Light load
- Trends
- Utilization
  - CPU
  - Disk
  - Network traffic
  - Memory
- Dashboard

5.2 Given a scenario, use the appropriate tool to identify server issues.

- Physical
  - Crash cart
  - Digital thermometer
  - KVM
  - Server manual
- Logical
  - Network tools
    - Nmap
    - nslookup
    - ipconfig/ifconfig/ip
    - ping
    - traceroute/tracert
    - dig
    - TCPView
    - arp
    - telnet
    - ssh
    - tnc
    - RDP/mstsc
    - curl
  - Process monitoring tools
    - Performance Monitor (perfmon)
    - Task Manager
    - top
    - Processview
  - Editor tools
    - vi
    - Notepad
  - File tools
    - Secure Hash Algorithm (SHA)
    - MD5
    - ls
    - dir
    - cat
  - Storage tools
    - DiskPart
    - fdisk
    - df
    - CHKDSK

5.3 Given a scenario, troubleshoot common hardware issues.

- Predictive failures
- Memory errors and failures
  - Registration
  - System crash
  - Blue screen
  - Purple screen
  - Memory dump
- Complementary metal-oxide-semiconductor (CMOS) battery
- Cache battery
- Auditory or olfactory cues
- Power-on self-test (POST) codes
- CPU or GPU overheating
- Faulty power supply
- Overheating

5.4 Given a scenario, troubleshoot common OS and software issues.

- Memory leak
- Corrupted file
- OS not loading
- Synchronization issues
- Encryption mismatch
- Configuration issues
- Logon issues
- Unresponsive application
- Degraded performance
- Driver issues
- Patch update failure

5.5 Given a scenario, troubleshoot common storage-related issues.

- RAID degradation
- Drive failure
- Cache battery failure
- Insufficient disk space
- Missing drive
- Degraded input/output (I/O) performance
- Read/write errors
- Unable to mount external devices
- Missing data
- Startup errors
- Data corruption
- Restore failure
- Unexpected encryption

5.6 Given a scenario, troubleshoot common network connectivity issues.

- Unable to join directory services
- Unable to access network resources
- Unavailable services
- Bad cable
- Connectivity issues
- Name resolution failure
- DHCP issues
- IP address conflicts

5.7 Given a scenario, troubleshoot common security issues.

- Login issues
- Permission issues
- Open ports
- Services
  - Active
  - Inactive
  - Orphan/zombie
- Rogue processes/services
- Unauthorized access
- File integrity issues
- Privilege escalation
- Data loss
- Redirection
- Traffic interception

CompTIA Server+ SK0-006 Acronym List

The following is a list of acronyms that appear on the CompTIA Server+ SK0-006 V6 certification exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as part of a comprehensive exam preparation program.

ACRONYM	DEFINITION
ACL	access control list
AD	Active Directory
APIPA	Automatic Private IP [Internet Protocol] Addressing
BC	business continuity
BCP	business continuity plan
BIA	business impact analysis
BIOS	Basic Input/Output System
BSOD	blue screen of death
CA	certificate authority
CIDR	Classless Inter-Domain Routing
CIFS	Common Internet File System
CIMC	Cisco Integrated Management Controller
CIS	Center for Internet Security
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	direct current
DDoS	distributed denial of service
DHCP	Dynamic Host Configuration Protocol
DLP	data loss prevention
DLT	Digital Linear Tape
DMZ	demilitarized zone
DNS	Domain Name System
DR	disaster recovery
DSC	Desired State Configuration
DSL	digital subscriber line
DVD	digital versatile disc
ECC	error-correcting code
EFS	Encrypting File System
eSATA	External Serial Advanced Technology Attachment

ACRONYM	DEFINITION
ESD	electrostatic discharge
FAT	File Allocation Table
FC-NVMe	NVMe [Non-Volatile Memory Express] over Fibre Channel
FCoE	Fibre Channel over Ethernet
FQDN	fully qualified domain name
FRU	field-replaceable unit
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
GFS	grandfather-father-son
GPO	Group Policy Object
GPT	GUID [globally unique identifier] Partition Table
GPU	graphics processing unit
GUI	graphical user interface
GUID	globally unique identifier
HBA	host bus adapter
HCL	hardware compatibility list
HDD	hard disk drives
HID	human interface device
HIDS	host-based intrusion detection system
HIPS	host-based intrusion prevention system
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	heating, ventilation, and air conditioning
IaaS	infrastructure as a service
IaC	infrastructure as code
IAM	identity and access management
IDF	intermediate distribution frame
iDRAC	Integrated Dell Remote Access Controller
IDS	intrusion detection system
IIS	Internet Information Services
iLO	Integrated Lights-Out
IMAP4	Internet Message Access Protocol 4
Intel-VT	Intel Virtualization Technology
I/O	input/output
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
iSCSI	Internet Small Computer System Interface
ISO	International Organization for Standardization
JBOD	just a bunch of disks

ACRONYM	DEFINITION
KVM	Keyboard-Video-Mouse
LAN	local area network
LC	Lucent 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
MBR	master boot record
MDF	main distribution frame
MFA	multifactor authentication
MIB	Management Information Base
MMC	Microsoft Management Console
MPO	multifiber push on
MRU	Most Recently Used
MSTSC	Microsoft Terminal Services Client
MTBF	mean time between failures
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
NPS	Network Policy Server
NTFS	New Technology File System
NTP	Network Time Protocol
NVMe	Non-Volatile Memory Express
OEM	original equipment manufacturer
OpenSCAP	Open Security Content Automation Protocol
OS	operating system
OSFP	Octal Small Form-factor Pluggable
OTP	one-time password
OU	organizational units
P2V	physical to virtual
PaaS	platform as a service
PAT	Port Address Translation

ACRONYM	DEFINITION
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
PPE	personal protective equipment
PQC	post-quantum cryptography
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 independent disks
RAM	random-access memory
RAS	remote access server
RDIMM	Registered Dual In-line Memory Module
RDP	Remote Desktop Protocol
ReFS	Resilient File System
RFC	Request for Comments
RFID	radio frequency identification
RIS	Remote Installation Services
RJ45	Registered Jack 45
RPM	revolutions per minute
RPO	recovery point objective
RTO	recovery time objective
SaaS	software as a service
SAN	storage area network
SAS	Serial Attached SCSI [Small Computer System Interface]
SATA	Serial Advanced Technology Attachment
SBOM	software bill of materials
SC	standard connector
SCCM	System Center Configuration Manager
SCP	Secure Copy Protocol
SCSI	Small Computer System Interface
SD	Secure Digital
SDS	safety data sheet
SELinux	Security-enhanced Linux
SFP	Small Form-factor Pluggable
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SLA	service-level agreement

ACRONYM	DEFINITION
SMS	Short Message Service
SMTP	Simple Mail Transfer 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
STIG	Security Technical Implementation Guide
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
UDIMM	Unbuffered Dual In-line Memory Module
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UID	Unique Identifier
UPS	uninterruptible power supply
URL	uniform resource locator
USB	Universal Serial Bus
UUID	Universally Unique Identifier
V2V	virtual to virtual
VAC	volts alternating current
VBS	Visual Basic Script
VDC	volts direct current
VLAN	virtual local area network
VM	virtual machine
VMFS	Virtual Machine File System
VNC	Virtual Network Computing
vNIC	virtual network interface card
VoIP	Voice over IP [Internet Protocol]
VPN	virtual private network
VSS	Volume Shadow Copy Service
VT	Virtualization Technology
WAN	wide area network
WDS	Windows Deployment Services
WINS	Windows Internet Naming Service
WMI	Windows Management Instrumentation
WOL	Wake-on-LAN
WSUS	Windows Software Update Services

ACRONYM	DEFINITION
WWNN	World Wide Node Name
WWPN	World Wide Port Name
XD	Execute Disable
ZFS	Z file system

CompTIA Server+ SK0-006 Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the Server+ SK0-006 V6 certification 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 sample lists and are not exhaustive.

HARDWARE

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

*Ideal, but not necessary for lab setup

SOFTWARE

- Cloud subscription
- Server OS
- Virtualization software
- Antivirus/anti-malware
- AI tool or assistant
- Automation tool(s)
- Log analysis tool(s)