CompTIA Server+ Certification Exam Objectives

EXAM NUMBER: SK0-005
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 SKo-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.

<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>PERCENTAGE OF EXAMINATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Server Hardware Installation and Management</td>
<td>18%</td>
</tr>
<tr>
<td>2.0 Server Administration</td>
<td>30%</td>
</tr>
<tr>
<td>3.0 Security and Disaster Recovery</td>
<td>24%</td>
</tr>
<tr>
<td>4.0 Troubleshooting</td>
<td>28%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
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

- **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)

- **Capacity planning**

- **Hard drive media types**
  - Solid state drive (SSD)
  - Wear factors
    - Read intensive

- **Interface types**
  - Serial attached SCSI (SAS)
  - Serial ATA (SATA)
  - Peripheral component interconnect (PCI)

- **Write intensive**
  - Hard disk drive (HDD)
    - Rotations per minute (RPM)
      - 15,000
      - 10,000
      - 7,200
    - Hybrid

- **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)
1.0 Server Hardware Installation and Management

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.

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

- Server roles requirements
  - Print
  - Database
  - File
  - Web
  - Application
  - Messaging
  - Baselining
    - Documentation
    - Performance metrics
- Monitoring
  - Disk quotas
  - Compression
  - Deduplication
- 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

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

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

- 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)
3.0 Security and Disaster Recovery

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

- **Mitigation strategies**
  - Breaches
    - Identification
    - Disclosure
  - Data monitoring
  - Log analysis
    - Security information and event management (SIEM)
  - Two-person integrity
    - Split encryption keys tokens
    - Separation of roles
  - 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**
- **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
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

- **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

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

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