EDUSUM

#1 Online Certification Guide

COMPTIA SK0-004

CompTIA Server+ Certification Questions & Answers

Exam Summary – Syllabus –Questions

SK0-004

CompTIA Server+

100 Questions Exam – 750/900 Cut Score – Duration of 90 minutes

Table of Contents:

Know Your SK0-004 Certification Well:

The SK0-004 is best suitable for candidates who want to gain knowledge in the CompTIA Infrastructure. Before you start your SK0-004 preparation you may struggle to get all the crucial Server+ materials like SK0-004 syllabus, sample questions, study guide.

But don't worry the SK0-004 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the SK0-004 syllabus?
- How many questions are there in the SK0-004 exam?
- Which Practice test would help me to pass the SK0-004 exam at the first attempt?

Passing the SK0-004 exam makes you CompTIA Server+. Having the Server+ certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

CompTIA SK0-004 Server+ Certification Details:

Exam Name	CompTIA Server+
Exam Code	SK0-004
Exam Price	$338 (USD)
Duration	90 mins
Number of Questions	100
Passing Score	750 / 900
Schedule Exam	**CompTIA Marketplace**
Sample Questions	**CompTIA Server+ Sample Questions**
Practice Exam	**CompTIA SK0-004 Certification Practice Exam**

SK0-004 Syllabus:

Topic	Details
Server Architecture - 12%	
Explain the purpose and function of server form factors.	1. Rack mount • Dimensions 1U, 2U, 4U • Cable management arms • Rail kits 2. Tower 3. Blade technology • Blade enclosure Backplane/midplane Power supply sockets Network modules/switches Management modules • Blade server
Given a scenario, install, configure and maintain server components.	1. CPU • Multiprocessor vs. multicore • Socket type • Cache levels: L1, L2, L3 • Speeds Core Bus Multiplier • CPU stepping • Architecture x86 x64 ARM 2. RAM • ECC vs. non-ECC • DDR2, DDR3 • Number of pins • Static vs. dynamic • Module placement

Topic	Details
	• CAS latency • Timing • Memory pairing 3. Bus types, bus channels and expansion slots • Height differences and bit rate differences • PCI • PCIe • PCI-X 4. NICs 5. Hard drives 6. Riser cards 7. RAID controllers 8. BIOS/UEFI • CMOS battery 9. Firmware 10. USB interface/port 11. Hotswap vs. non-hotswap components
Compare and contrast power and cooling components.	1. 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 2. Cooling • Airflow • Thermal dissipation • Baffles/shrouds • Fans • Liquid cooling

Topic	Details
Server Administration - 24%	
Install and configure server operating systems.	1. Determine server role/purpose 2. Update firmware 3. BIOS/UEFI configuration • Boot order 4. Disk preparation • RAID setup • Partitioning • Formatting • File system type Ext 2, 3, 4 NTFS FAT32 ReiserFS UFS VMFS ZFS • Swap 5. Configure host name 6. Local account setup 7. Connect to network 8. Join domain/directory 9. Address security concerns • Patching • OS hardening • Compliance to company procedures/standards 10. Enable services 11. Install features/roles/applications/drivers 12. Performance baseline • Server optimization • Swap or pagefile optimization 13. Unattended/remote installations • Deploying images and cloning

Topic	Details
	• Scripted installs PXE boot TFTP
Compare and contrast server roles and requirements for each.	1. Web server 2. Application server 3. Directory server 4. Database server 5. File server 6. Print server 7. Messaging server 8. Mail server 9. Routing and remote access server 10. Network services server • DHCP • DNS/WINS • NTP
Given a scenario, use access and control methods to administer a server.	1. Local hardware administration • KVM • Serial • Virtual administration console 2. Network-based hardware administration • KVM over IP • ILO • iDRAC 3. Network-based operating system administration • RDP • SSH • VNC • Command line/shell
Given a scenario, perform proper server maintenance techniques.	1. Change management 2. Patch management • Operating system updates • Application updates • Security software updates

Topic	Details
	• Firmware updates • Device drivers updates • Compatibility lists Operating systems Hardware Applications • Testing and validation 3. Outages and service level agreements • Scheduled downtime • Unscheduled downtime • Impact analysis • Client notification • MTTR 4. Performance monitoring • CPU utilization • Memory utilization • Network utilization • Disk utilization Disk IOPS Storage capacity • Comparison against performance baseline • Processes and services monitoring • Log monitoring 5. Hardware maintenance • Check system health indicators LEDs Error codes Beep codes LCD messages • Replace failed components Fans Hard drives RAM Backplanes Batteries • Preventive maintenance Clearing dust Check proper air flow

Topic	Details
	• Proper shut down procedures 6. Fault tolerance and high availability techniques • Clustering Active/active Active/passive • Load balancing Round robin Heartbeat
Explain the importance of asset management and documentation.	1. Asset management • Licensing • Labeling • Warranty • Life cycle management Procurement Usage End of life Disposal/recycling • Inventory Make Model Serial number Asset tag 2. Documentation • Service manuals • Network diagrams • Architecture diagrams • Dataflow diagrams • Recovery documentation • Baseline documentation • Change management policies • Service level agreement • Server configuration 3. Secure storage of sensitive documentation
Explain the purpose and operation of virtualization components.	1. Hosts and guests 2. Management interface for virtual machines 3. Hypervisor • Type I

Topic	Details
	• Type II • Hybrid 4. Hardware compatibility list • BIOS/UEFI compatibility and support • CPU compatibility support • AMD-V/Intel VT 5. Resource allocation between guest and host • CPU • Storage • Memory • Network connectivity Direct access (bridging) vs. NAT Virtual NICs Virtual switches • Video
Storage - 12%	
Given a scenario, install and deploy primary storage devices based on given specifications and interfaces.	1. Disk specifications • RPM • Dimensions/form factor • Capacity • Bus width • IOPS • Seek time and latency • Hotswap vs. non-hotswap components 2. Interfaces • SAS • SATA • SCSI • USB • Fibre channel 3. Hard drive vs. SSD
Given a scenario, configure RAID using best practices.	1. RAID levels and performance considerations • 0

Topic	Details
	• 1 • 5 • 6 • 10 2. Software vs. hardware RAID • Performance considerations 3. Configuration specifications • Capacity • Bus types • Drive RPM 4. Hotswap support and ramifications 5. Hot spare vs. cold spare 6. Array controller • Memory • Battery backed cache • Redundant controller
Summarize hardware and features of various storage technologies.	1. DAS 2. NAS • CIFS/SMB • NFS 3. SAN • iSCSI • FCoE • Fibre channel • LUN and LUN masking • HBAs and fabric switches 4. JBOD 5. Tape • Drive • Libraries 6. Optical drive 7. Flash, compact flash and USB drive

Topic	Details
Given a scenario, calculate appropriate storage capacity and plan for future growth.	1. Base10 vs. Base2 disk size calculation (1000 vs. 1024) 2. Disk quotas 3. Compression 4. Capacity planning considerations • Operating system growth Patches Service packs Log files Temporary directories Databases Application servers File servers Archival
Security - 13%	
Compare and contrast physical security methods and concepts.	1. Multifactor authentication • Something you have • Something you know • Something you are 2. Security concepts • Mantrap • RFID chip • ID card • Biometric • Keypad • Access list • Security guard • Security camera • Keys and locks Cabinet Rack mount Server • Safe
Given a scenario, apply server hardening techniques.	1. OS hardening • Stopping unneeded services/ closing unneeded ports • Install only required software • Install latest operating system patches

Topic	Details
	2. Application hardening • Install latest patches • Disabling unneeded services/roles/features 3. Endpoint security • HIDS • Anti-malware 4. Remediate security issues based on a vulnerability scan 5. Hardware hardening • Disabling unneeded hardware and physical ports/devices • BIOS password • Disable WOL (Wake on LAN) • Setup boot order • Chassis locks/intrusion detection
Explain basic network security systems and protocols.	1. Firewall • Network-based • Host-based 2. Port security/802.1x/NAC 3. Router access list 4. NIDS 5. Authentication protocols • LDAP • RADIUS • TACACS • TACACS+ 6. PKI • Private key • Public key • Certificate authority • SSL/TLS 7. VPN 8. IPSec

Topic	Details
	9. VLAN 10. Security zones • DMZ • Public and private • Intranet and extranet
Implement logical access control methods based on company policy.	1. ACLs • Users • Groups Roles • Resources File system Network ACLs Peripheral devices Administrative rights Distribution lists 2. Permissions • Read • Write/modify • Execute • Delete • Full control/superuser • File vs. share
Implement data security methods and secure storage disposal techniques.	1. Storage encryption • File level encryption • Disk encryption • Tape encryption 2. Storage media • Soft wipe File deletion • Hard wipe Zero out all sectors Physical destruction Remote wipe
Given a scenario, implement proper	1. Power concepts and best practices

Topic	Details
environmental controls and techniques.	• 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 2. Safety • ESD procedures • Fire suppression • Proper lifting techniques • Rack stability • Floor load limitations • Sharp edges and pinch points 3. HVAC • Room and rack temperature and humidity Monitoring and alert notifications • Air flow Rack filler/baffle/blanking panels • Hot aisle and cold aisle
Networking - 10%	
Given a scenario, configure servers to use IP addressing and network infrastructure services.	1. IPv4 vs. IPv6 2. Default gateway 3. CIDR notation and subnetting 4. Public and private IP addressing 5. Static IP assignment vs. DHCP 6. DNS • FQDN

Topic	Details
	• Default domain suffix/search domain 7. WINS 8. NetBIOS 9. NAT/PAT 10. MAC addresses 11. Network Interface Card configuration • NIC teaming • Duplexing Full Half Auto • Speeds 10/100/1000 Mbps 10 Gbps
Compare and contrast various ports and protocols.	1. TCP vs. UDP 2. SNMP 161 3. SMTP 25 4. FTP 20/21 5. SFTP 22 6. SSH 22 7. SCP 22 8. NTP 123 9. HTTP 80 10. HTTPS 443 11. TELNET 23 12. IMAP 143 13. POP3 110 14. RDP 3389 15. FTPS 989/990 16. LDAP 389/3268 17. DNS 53 18. DHCP 67/68
Given a scenario, install cables and implement proper cable management procedures.	1. Copper • Patch cables Crossover Straight through Rollover 2. Fiber • Single mode

Topic	Details
	• Multimode 3. Connectors • ST • LC • BNC • SC • SFP • RJ-45 • RJ-11 4. Cable placement and routing • Cable channels • Cable management trays Vertical Horizontal 5. Labeling 6. Bend radius 7. Plenum cables 8. Cable ties
Disaster Recovery - 9%	
Explain the importance of disaster recovery principles.	1. Site types • Hot site • Cold site • Warm site 2. Replication methods • Disk-to-disk • Server-to-server • Site-to-site 3. Continuity of operations • Disaster recovery plan • Business continuity plan • Business impact analysis Who is affected What is affected Severity of impact

Topic	Details
Given a scenario, implement appropriate backup techniques.	1. Methodology • Full/normal Copy • Incremental • Differential • Snapshot • Selective • Bare metal • Open file • Data vs. OS restore 2. Backup media • Linear access Tape • Random access Disk Removable media Optical media 3. Media and restore best practices • Labeling • Integrity verification • Test restorability • Tape rotation and retention 4. Media storage location • Offsite • Onsite • Security considerations • Environmental considerations
Troubleshooting - 20%	
Explain troubleshooting theory and methodologies.	1. 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

Topic	Details
	• If possible, perform backups before making changes 2. Establish a theory of probable cause (question the obvious) • Determine whether there is a common element of symptom causing multiple problems 3. 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 4. Establish a plan of action to resolve the problem and notify impacted users 5. 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 6. Verify full system functionality and if applicable implement preventative measures 7. Perform a root cause analysis 8. Document findings, actions and outcomes throughout the process
Given a scenario, effectively troubleshoot hardware problems, selecting the appropriate tools and methods.	1. 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 2. Causes of common problems • Third-party components or incompatible components

Topic	Details
	• Incompatible or incorrect BIOS • Cooling failure • Mismatched components • Backplane failure 3. Environmental issues • Dust • Humidity • Temperature • Power surge/failure 4. Hardware tools • Power supply tester (multimeter) • Hardware diagnostics • Compressed air • ESD equipment
Given a scenario, effectively troubleshoot software problems, selecting the appropriate tools and methods.	1. Common problems • User unable to log on • 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 2. Cause of common problems • User Account Control (UAC/SUDO) • Corrupted files • Lack of hard drive space • Lack of system resources

Topic	Details
	• Virtual memory (misconfigured, corrupt) • Fragmentation • Print server drivers/services • Print spooler 3. Software tools • System logs • Monitoring tools (resource monitor, performance monitor) • Defragmentation tools • Disk property tools (usage, free space, volume or drive mapping)
Given a scenario, effectively diagnose network problems, selecting the appropriate tools and methods.	1. Common problems • Internet connectivity failure • Email failure • Resource unavailable • DHCP server misconfigured • Non-functional or unreachable • Destination host unreachable • Unknown host • Default gateway misconfigured • Failure of service provider • Cannot reach by host name/FQDN 2. Causes of common problems • Improper IP configuration • VLAN configuration • Port security • Improper subnetting • Component failure • Incorrect OS route tables • Bad cables • Firewall (misconfiguration, hardware failure, software failure) • Misconfigured NIC, routing/switch issues • DNS and/or DHCP failure • Misconfigured hosts file

Topic	Details
	• IPv4 vs. IPv6 misconfigurations 3. Networking tools • ping • tracert/traceroute • ipconfig/ifconfig • nslookup • net use/mount • route • nbtstat • netstat
Given a scenario, effectively troubleshoot storage problems, selecting the appropriate tools and methods.	1. 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 2. Causes of common problems • Media failure • Drive failure • Controller failure • HBA failure • Loose connectors • Cable problems • Misconfiguration • Improper termination • Corrupt boot sector

Topic	Details
	• Corrupt file system table • Array rebuild • Improper disk partition • Bad sectors • Cache battery failure • Cache turned off • Insufficient space • Improper RAID configuration • Mismatched drives • Backplane failure 3. Storage tools • Partitioning tools • Disk management • RAID array management • Array management • System logs • Net use/mount command • Monitoring tools
Given a scenario, effectively diagnose security issues, selecting the appropriate tools and methods.	1. Common problems • File integrity issue • Privilege escalation • Applications will not load • Cannot access network file/shares • Unable to open files • Excessive access • Excessive memory utilization 2. Causes of common problems • Open ports • Active services • Inactive services • Intrusion detection configurations • Anti-malware configurations • Local/group policies • Firewall rules

Topic	Details
	• Misconfigured permissions • Virus infection • Rogue processes/services 3. Security tools • Port scanners • Sniffers • Cipher • Checksums • Telnet client • Anti-malware

CompTIA SK0-004 Sample Questions:

Question: 1

Which of the following should an administrator utilize when installing a new server to ensure that best practices are followed?

a) Service Level Agreement (SLA)
b) Warranty regulations
c) Vendor support documentation
d) Equipment disposal policies

Answer: c

Question: 2

An administrator recently performed a NIC driver upgrade on several servers and now is seeing lost packets and some disconnected switches. Which of the following is the BEST course of action to resolve this issue?

a) Restart the server and see if the issue still remains. If the issue still exists open a case with the OEM of the NIC.
b) Call the OEM of the NIC and open a case with them to investigate the issue. Roll back the NIC driver to the previous working revision.
c) Call the OEM of the NIC and open a case with them to investigate the issue.
d) Go to the OEM's website and download another NIC driver to test.

Answer: b

Question: 3

Which of the following involves the copying off and removal of data from file servers?

a) Backing up
b) Archiving
c) Recovery
d) Replicating

Answer: b

Question: 4

Which of the following ways can a technician use to see if a server is under warranty?

a) Escalate the problem to upper management.
b) Assume the part is no longer under warranty, and order a replacement part.
c) Perform a root cause analysis.
d) Contact the OEM to verify the warranty status, and then document the findings.

Answer: d

Question: 5

As a best practice, in which of the following locations should antivirus software be installed?

a) Only on the administrator's workstation
b) Only on the domain controller
c) Only on the general manager's workstation
d) On all servers
e) On all workstations

Answer: d, e

Question: 6

Which of the following expansion cards should be installed to give a server FireWire connectivity?

a) IEEE 802.11
b) NIC
c) HBA
d) IEEE 1394

Answer: d

Question: 7

Which of the following BEST describes an HCL?

a) A list of permissions for network access and routing
b) A list of approved hardware
c) A list of permissions for file sharing
d) A method of attaching a server to a SAN

Answer: b

Question: 8

Which of the following is a benefit of hot-swappable parts?

a) Ability to utilize logical unit numbers (LUNs)
b) Ability to implement USB devices
c) Ability to utilize flash memory
d) Ability to replace hardware without interrupting the server's power

Answer: d

Question: 9

Which of the following file systems is native to an ESX server?

a) NTFS
b) EXT3
c) FAT32
d) VMFS

Answer: d

Question: 10

Which of the following expansion card ports is the fastest?

a) ISA
b) PCI
c) PCIx
d) PCIe

Answer: d

Study Guide to Crack CompTIA Server+ SK0-004 Exam:

- Getting details of the SK0-004 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the SK0-004 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the CompTIA provided training for SK0-004 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the SK0-004 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on SK0-004 practice tests is must. Continuous practice will make you an expert in all syllabus areas.