EDUSUM

#1 Online Certification Guide

COMPTIA SK0-005

CompTIA Server+ Certification Questions & Answers

Exam Summary – Syllabus –Questions

SK0-005

CompTIA Server+

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

Table of Contents:

Know Your SK0-005 Certification Well:

The SK0-005 is best suitable for candidates who want to gain knowledge in the CompTIA Infrastructure. Before you start your SK0-005 preparation you may struggle to get all the crucial Server+ materials like SK0-005 syllabus, sample questions, study guide.

But don't worry the SK0-005 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 SK0-005 syllabus?
- How many questions are there in the SK0-005 exam?
- Which Practice test would help me to pass the SK0-005 exam at the first attempt?

Passing the SK0-005 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 SK0-005 Server+ Certification Details:

Exam Name	CompTIA Server+
Exam Code	SK0-005
Exam Price	$338 (USD)
Duration	90 mins
Number of Questions	90
Passing Score	750 / 900
Schedule Exam	**CompTIA Marketplace** **Pearson VUE**
Sample Questions	**CompTIA Server+ Sample Questions**
Practice Exam	**CompTIA SK0-005 Certification Practice Exam**

SK0-005 Syllabus:

Topic	Details
Server Hardware Installation and Management - 18%	
Given a scenario, install physical hardware.	- Racking 1. Enclosure sizes 2. Unit sizes - 1U, 2U, 3U, etc. 3. Rack layout - Cooling management - Safety 1. Proper lifting techniques 2. Rack balancing 3. Floor load limitations - Power distribution unit (PDU) - Keyboard-video-mouse (KVM) placement - Rail kits - Power cabling 1. Redundant power - Uninterruptible power supply (UPS) - Separate circuits - Separate providers 2. Power connector types 3. Cable management - Network cabling 1. Redundant networking 2. Twisted pair 3. Fiber - SC - LC - Single mode - Multimode 4. Gigabit 5. 10 GigE 6. Small form factor pluggable (SFP) 7. SFP+ 8. Quad small form factor pluggable (QSFP) 9. Cable management - Server chassis types

Topic	Details
	1. Tower 2. Rack mount 3. Blade enclosure - Server components 1. Hardware compatibility list (HCL) 2. Central processing unit (CPU) 3. Graphics processing unit (GPU) 4. Memory 5. Bus types 6. Interface types 7. Expansion cards
Given a scenario, deploy and manage storage.	- RAID levels and types 1. 0 2. 1 3. 5 4. 6 5. 10 6. Just a bunch of disks (JBOD) 7. Hardware vs. software - Capacity planning - Hard drive media types 1. Solid state drive (SSD) - Wear factors 1. Read intensive 2. Write intensive 2. Hard disk drive (HDD) - Rotations per minute (RPM) 1. 15,000 2. 10,000 3. 7,200 3. Hybrid - Interface types 1. Serial attached SCSI (SAS) 2. Serial ATA (SATA) 3. Peripheral component interconnect (PCI) 4. External serial advanced technology attachment (eSATA) 5. Universal serial bus (USB)

Topic	Details
	6. Secure digital (SD) - Shared storage 1. Network attached storage (NAS) - Network file system (NFS) - Common Internet file system (CIFS) 2. Storage area network (SAN) - Internet small computer systems interface (iSCSI) - Fibre Channel - Fibre Channel over Ethernet (FCoE)
Given a scenario, perform server hardware maintenance.	- Out-of-band management 1. Remote drive access 2. Remote console access 3. Remote power on/off 4. Internet protocol keyboard-video-mouse (IP KVM) - Local hardware administration 1. Keyboard-video-mouse (KVM) 2. Crash cart 3. Virtual administration console 4. Serial connectivity 5. Console connections - Components 1. Firmware upgrades - Drives - Hot-swappable hardware 1. Drives 2. Cages 3. Cards 4. Power supplies 5. Fans - Basic input/output system (BIOS)/Unified Extensible Firmware Interface (UEFI)

Topic	Details
Server Administration - 30%	
Given a scenario, install server operating systems.	- Minimum operating system (OS) requirements - Hardware compatibility list (HCL) - Installations 1. Graphical user interface (GUI) 2. Core 3. Bare metal 4. Virtualized 5. Remote 6. Slip streamed/unattended - Scripted installations - Additional drivers - Additional applications and utilities - Patches 7. Media installation type - Network - Optical - Universal serial bus (USB) - Embedded 8. Imaging - Cloning 1. Virtual machine (VM) cloning 2. Physical clones 3. Template deployment 4. Physical to virtual (P2V) - Partition and volume types 1. Global partition table (GPT) vs. master boot record (MBR) 2. Dynamic disk 3. Logical volume management (LVM) - File system types 1. ext4 2. New technology file system (NTFS) 3. VMware file system (VMFS) 4. Resilient file system (ReFS) 5. Z file system (ZFS)
Given a scenario, configure servers to use	- IP configuration - Virtual local area network (VLAN)

Topic	Details
network infrastructure services.	- Default gateways - Name resolution 1. Domain name service (DNS) 2. Fully qualified domain name (FQDN) 3. Hosts file - Addressing protocols 1. IPv4 - Request for comments (RFC) 1918 address spaces 2. IPv6 - Firewall 1. Ports - Static vs. dynamic 1. Dynamic host configuration protocol (DHCP) - MAC addresses
Given a scenario, configure and maintain server functions and features.	- Server roles requirements 1. Print 2. Database 3. File 4. Web 5. Application 6. Messaging 7. Baselining - Documentation - Performance metrics - Directory connectivity - Storage management 1. Formatting 2. Connectivity 3. Provisioning 4. Partitioning 5. Page/swap/scratch location and size 6. Disk quotas 7. Compression

Topic	Details
	8. Deduplication - Monitoring 1. Uptime 2. Thresholds 3. Performance - Memory - Disk 1. Input output operations per second (IOPS) 2. Capacity vs. utilization - Network - Central processing unit (CPU) 4. Event logs - Configuration - Shipping - Alerting - Reporting - Retention - Rotation - Data migration and transfer 1. Infiltration 2. Exfiltration 3. Disparate OS data transfer - Robocopy - File transfer - Fast copy - Secure copy protocol (SCP) - Administrative interfaces 1. Console 2. Remote desktop 3. Secure shell (SSH) 4. Web interface
Explain the key concepts of high availability for servers.	- Clustering 1. Active-active 2. Active-passive 3. Failover 4. Failback 5. Proper patching procedures 6. Heartbeat

Topic	Details
	- Fault tolerance 1. Server-level redundancy vs. component redundancy - Redundant server network infrastructure 1. Load balancing - Software vs. hardware - Round robin - Most recently used (MRU) 2. Network interface card (NIC) teaming and redundancy - Failover - Link aggregation
Summarize the purpose and operation of virtualization.	- Host vs. guest - Virtual networking 1. Direct access (bridged) 2. Network address translation (NAT) 3. vNICs 4. Virtual switches - Resource allocation and provisioning 1. CPU 2. Memory 3. Disk 4. NIC 5. Overprovisioning 6. Scalability - Management interfaces for virtual machines - Cloud models 1. Public 2. Private 3. Hybrid
Summarize scripting basics for server administration.	- Script types 1. Bash 2. Batch 3. PowerShell 4. Virtual basic script (VBS)

Topic	Details
	- Environment variables - Comment syntax - Basic script constructs 1. Loops 2. Variables 3. Conditionals 4. Comparators - Basic data types 1. Integers 2. Strings 3. Arrays - Common server administration scripting tasks 1. Startup 2. Shut down 3. Service 4. Login 5. Account creation 6. Bootstrap
Explain the importance of asset management and documentation.	- Asset management 1. Labeling 2. Warranty 3. Leased vs. owned devices 4. Life-cycle management - Procurement - Usage - End of life - Disposal/recycling 5. Inventory - Make - Model - Serial number - Asset tag - Documentation management 1. Updates 2. Service manuals 3. Architecture diagrams 4. Infrastructure diagrams 5. Workflow diagrams

Topic	Details
	6. Recovery processes 7. Baselines 8. Change management 9. Server configurations 10. 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
Explain licensing concepts.	- Models 1. Per-instance 2. Per-concurrent user 3. Per-server 4. Per-socket 5. Per-core 6. Site-based 7. Physical vs. virtual 8. Node-locked 9. Signatures - Open source - Subscription - License vs. maintenance and support - Volume licensing - License count validation 1. True up - Version compatibility 1. Backward compatible 2. Forward compatible
Security and Disaster Recovery - 24%	
Summarize data security concepts.	- Encryption paradigms 1. Data at rest

Topic	Details
	2. Data in transit - Retention policies - Data storage 1. Physical location storage 2. Off-site vs. on-site - UEFI/BIOS passwords - Bootloader passwords - Business impact 1. Data value prioritization 2. Life-cycle management 3. Cost of security vs. risk and/or replacement
Summarize physical security concepts.	- Physical access controls 1. Bollards 2. Architectural reinforcements - Signal blocking - Reflective glass - Datacenter camouflage 3. Fencing 4. Security guards 5. Security cameras 6. Locks - Biometric - Radio frequency identification (RFID) - Card readers - Mantraps - Safes - Environmental controls 1. Fire suppression 2. Heating, ventilation, and cooling (HVAC) 3. Sensors
Explain important concepts pertaining to identity and access management for server administration.	- User accounts - User groups - Password policies 1. Length 2. Lockout

Topic	Details
	3. Enforcement - Permissions and access controls 1. Role-based 2. Rule-based 3. Scope based 4. Segregation of duties 5. Delegation - Auditing 1. User activity 2. Logins 3. Group memberships 4. Deletions - Multifactor authentication (MFA) 1. Something you know 2. Something you have 3. Something you are - Single sign-on (SSO)
Explain data security risks and mitigation strategies.	- Security risks 1. Hardware failure 2. Malware 3. Data corruption 4. Insider threats 5. Theft - Data loss prevention (DLP) - Unwanted duplication - Unwanted publication 6. Unwanted access methods - Backdoor - Social engineering 7. Breaches - Identification - Disclosure - Mitigation strategies 1. Data monitoring 2. Log analysis - Security information and event management (SIEM)

Topic	Details
	3. Two-person integrity - Split encryption keys tokens - Separation of roles 4. Regulatory constraints - Governmental - Individually privileged information 1. Personally identifiable information (PII) 2. Payment Card Industry DataSecurity Standard (PCI DSS) 5. Legal considerations - Data retention - Subpoenas
Given a scenario, apply server hardening methods.	- OS hardening 1. Disable unused services 2. Close unneeded ports 3. Install only required software 4. Apply driver updates 5. Apply OS updates 6. Firewall configuration - Application hardening 1. Install latest patches 2. Disable unneeded services, roles, or features - Host security 1. Antivirus 2. Anti-malware 3. Host intrusion detection system (HIDS)/Host intrusion prevention system (HIPS) - Hardware hardening 1. Disable unneeded hardware 2. Disable unneeded physical ports, devices, or functions 3. Set BIOS password 4. Set boot order - Patching 1. Testing 2. Deployment

Topic	Details
	3. Change management
Summarize proper server decommissioning concepts.	- Proper removal procedures 1. Company policies 2. Verify non-utilization 3. Documentation - Asset management - Change management - Media destruction 1. Disk wiping 2. Physical - Degaussing - Shredding - Crushing - Incineration 3. Purposes for media destruction - Media retention requirements - Cable remediation 1. Power 2. Networking - Electronics recycling 1. Internal vs. external 2. Repurposing
Explain the importance of backups and restores.	- Backup methods 1. Full 2. Synthetic full 3. Incremental 4. Differential 5. Archive 6. Open file 7. Snapshot - Backup frequency - Media rotation - Backup media types 1. Tape

Topic	Details
	2. Cloud 3. Disk 4. Print - File-level vs. system-state backup - Restore methods 1. Overwrite 2. Side by side 3. Alternate location path - Backup validation 1. Media integrity 2. Equipment 3. Regular testing intervals - Media inventory before restoration
Explain the importance of disaster recovery.	- Site types 1. Hot site 2. Cold site 3. Warm site 4. Cloud 5. Separate geographic locations - Replication 1. Constant 2. Background 3. Synchronous vs. asynchronous 4. Application consistent 5. File locking 6. Mirroring 7. Bidirectional - Testing 1. Tabletops 2. Live failover 3. Simulated failover 4. Production vs. non-production

Topic	Details
Troubleshooting - 28%	
Explain the troubleshooting theory and methodology.	- Identify the problem and determine the scope. 1. Question users/stakeholders and identify changes to the server/environment. 2. Collect additional documentation/logs. 3. If possible, replicate the problem as appropriate. 4. If possible, perform backups before making changes. 5. Escalate, if necessary. - Establish a theory of probable cause (question the obvious). 1. Determine whether there is a common element or symptom causing multiple problems. - Test the theory to determine the cause. 1. Once the theory is confirmed, determine the next steps to resolve the problem. 2. If the theory is not confirmed, establish a new theory. - Establish a plan of action to resolve the problem. 1. Notify impacted users. - Implement the solution or escalate. 1. Make one change at a time and test/confirm the change has resolved the problem. 2. 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.
Given a scenario, troubleshoot common hardware failures.	- Common problems 1. Predictive failures 2. Memory errors and failures - System crash 1. Blue screen 2. Purple screen

Topic	Details
	3. Memory dump - Utilization - Power-on self-test (POST) errors - Random lockups - Kernel panic 3. Complementary metal-oxide-semiconductor (CMOS) battery failure 4. System lockups 5. Random crashes 6. Fault and device indication - Visual indicators 7. Light-emitting diode (LED) 8. Liquid crystal display (LCD) panel readouts - Auditory or olfactory cues - POST codes 9. Misallocated virtual resources - Causes of common problems 1. 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 2. Environmental - Dust - Humidity - Temperature - Tools and techniques 1. Event logs 2. Firmware upgrades or downgrades 3. Hardware diagnostics 4. Compressed air 5. Electrostatic discharge (ESD) equipment 6. Reseating or replacing components and/or cables
Given a scenario, troubleshoot storage problems.	- Common problems 1. Boot errors 2. Sector block errors

Topic	Details
	3. Cache battery failure 4. Read/write errors 5. Failed drives 6. Page/swap/scratch file or partition 7. Partition errors 8. Slow file access 9. OS not found 10. Unsuccessful backup 11. Unable to mount the device 12. Drive not available 13. Cannot access logical drive 14. Data corruption 15. Slow I/O performance 16. Restore failure 17. Cache failure 18. Multiple drive failure - Causes of common problems 1. Disk space utilization - Insufficient disk space 2. Misconfigured RAID 3. Media failure 4. Drive failure 5. Controller failure 6. Hot bus adapter (HBA) failure 7. Loose connectors 8. Cable problems 9. Misconfiguration 10. Corrupt boot sector 11. Corrupt filesystem table 12. Array rebuild 13. Improper disk partition 14. Bad sectors 15. Cache battery failure 16. Cache turned off 17. Insufficient space 18. Improper RAID configuration 19. Mismatched drives 20. Backplane failure - Tools and techniques 1. Partitioning tools 2. Disk management 3. RAID and array management 4. System logs

Topic	Details
	5. Disk mounting commands - net use - mount 6. Monitoring tools 7. Visual inspections 8. Auditory inspections
Given a scenario, troubleshoot common OS and software problems.	- Common problems 1. Unable to log on 2. Unable to access resources 3. Unable to access files 4. System file corruption 5. End of life/end of support 6. Slow performance 7. Cannot write to system logs 8. Service failures 9. System or application hanging 10. Freezing 11. Patch update failure - Causes of common problems 1. Incompatible drivers/modules 2. Improperly applied patches 3. Unstable drivers or software 4. Server not joined to domain 5. Clock skew 6. Memory leaks 7. Buffer overrun 8. Incompatibility Insecure dependencies Version management Architecture 9. Update failures 10. Missing updates 11. Missing dependencies 12. Downstream failures due to updates 13. Inappropriate application-level permissions 14. Improper CPU affinity and priority - OS and software tools and techniques 1. Patching - Upgrades - Downgrades 2. Package management

Topic	Details
	3. Recovery - Boot options 1. Safe mode 2. Single user mode - Reload OS - Snapshots 4. Proper privilege escalations - runas/Run As - sudo - su 5. Scheduled reboots 6. Software firewalls - Adding or removing ports - Zones 7. Clocks - Network time protocol (NTP) - System time 8. Services and processes - Starting - Stopping - Status identification - Dependencies 9. Configuration management - System center configuration manager (SCCM) - Puppet/Chef/Ansible - Group Policy Object (GPO) 10. Hardware compatibility list (HCL)
Given a scenario, troubleshoot network connectivity issues.	- Common problems 1. Lack of Internet connectivity 2. Resource unavailable 3. Receiving incorrect DHCP information 4. Non-functional or unreachable 5. Destination host unreachable 6. Unknown host 7. Unable to reach remote subnets 8. Failure of service provider 9. Cannot reach server by hostname/fully qualified domain name (FQDN) - Causes of common problems 1. Improper IP configuration 2. IPv4 vs. IPv6 misconfigurations 3. Improper VLAN configuration 4. Network port security

Topic	Details
	5. Component failure 6. Incorrect OS route tables 7. Bad cables 8. Firewall (misconfiguration, hardware failure, software failure) 9. Misconfigured NIC 10. DNS and/or DHCP failure 11. DHCP server misconfigured 12. Misconfigured hosts file - Tools and techniques 1. Check link lights 2. Confirm power supply 3. Verify cable integrity 4. Check appropriate cable selection 5. Commands - ipconfig - ip addr - ping - tracert - traceroute - nslookup - netstat - dig - telnet - nc - nbtstat - route
Given a scenario, troubleshoot security problems.	- Common concerns 1. File integrity 2. Improper privilege escalation - Excessive access 3. Applications will not load 4. Cannot access network fileshares 5. Unable to open files - Causes of common problems 1. Open ports 2. Services - Active - Inactive - Orphan/zombie 3. Intrusion detection configurations

Topic	Details
	4. Anti-malware configurations 5. Improperly configured local/group policies - Improperly configured firewall rules 1. Misconfigured permissions 2. Virus infection 3. Malware 4. Rogue processes/services 5. Data loss prevention (DLP) - Security tools 1. Port scanners 2. Sniffers 3. Telnet clients 4. Anti-malware 5. Antivirus 6. File integrity - Checksums - Monitoring - Detection - Enforcement 7. User access controls - SELinux - User account control (UAC)

CompTIA SK0-005 Sample Questions:

Question: 1

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: 2

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: 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? (Choose two)

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 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: 8

Which of the following expansion card ports is the fastest?

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

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 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

Study Guide to Crack CompTIA Server+ SK0-005 Exam:

- Getting details of the SK0-005 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 SK0-005 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 SK0-005 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 SK0-005 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 SK0-005 practice tests is must. Continuous practice will make you an expert in all syllabus areas.