PROGRAMMA CompTIA Server + (SK0-005)

40 ore

1.0 Server Hardware Installation and Management

1.1 Install physical hardware.

• Racking- Enclosure sizes- Unit sizes- 1U, 2U, 3U, etc.- Rack layout- Cooling management- Safety- Proper lifting techniques- Rack balancing- Floor load limitations- Power distribution unit (PDU)- Keyboard-video- mouse (KVM) placement- Rail kits

• Power cabling- Redundant power- Uninterruptible power supply (UPS)- Separate circuits- Separate providers- Power connector types- Cable management

• Network cabling- Redundant networking- Twisted pair- Fiber- SC- LC- Single mode- Multimode- Gigabit- 10 GigE- Small form factor pluggable (SFP)- SFP+- Quad small form factor pluggable (QSFP)- Cable management

• Server chassis types- Tower- Rack mount- Blade enclosure

• Server components- Hardware compatibility list (HCL)- Central processing unit (CPU)- Graphics processing unit (GPU)- Memory- Bus types- Interface types- Expansion cards

1.2 Deploy and manage storage.

• RAID levels and types- 0- 1- 5- 6- 10- Just a bunch of disks (JBOD)- Hardware vs. software

• Capacity planning

• Hard drive media types- Solid state drive (SSD)- Wear factors- Read intensive- Write intensive- Hard disk drive (HDD)- Rotations per minute (RPM)- 15,000- 10,000- 7,200- Hybrid
• Interface types- Serial attached SCSI (SAS)- Serial ATA (SATA)- Peripheral component interconnect (PCI)- External serial advanced technology attachment (eSATA)- Universal serial bus (USB)- Secure digital (SD)
• Shared storage- Network attached storage (NAS)- Network file system (NFS)- Common Internet file system (CIFS)- Storage area network (SAN)- Internet small computer systems interface (iSCSI)- Fibre Channel- Fibre Channel over Ethernet (FCoE)

1.3 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 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 Configure servers to use network infrastructure services

• IP configuration

• Virtual local area network (VLAN)

• Default gateways

• Name resolution- Domain name service (DNS)- Fully qualified domain name (FQDN)- Hosts file

• Addressing protocols- IPv4- Request for comments (RFC) 1918 address spaces- IPv6• Firewall- Ports

• Static vs. dynamic- Dynamic host configuration protocol (DHCP)- Automatic private IP address (APIPA)

• MAC addresses

2.3 Configure and maintain server functions and features.

• Server roles requirements- Print- Database- File- Web- Application- Messaging- Baselining- Documentation- Performance metrics

• Directory connectivity

• Storage management- Formatting- Connectivity- Provisioning- Partitioning- Page/swap/scratch location and size- Disk quotas- Compression- Deduplication

• Monitoring- Uptime- Thresholds - Performance - Memory - Disk- Input output operations per second (IOPS)- Capacity vs. utilization - Network- Central processing unit (CPU)- Event logs - Configuration - Shipping - Alerting - Reporting - Retention - Rotation

• Data migration and transfer- Infiltration- Exfiltration- Disparate OS data transfer - Robocopy- File transfer- Fast copy- Secure copy protocol (SCP)

• Administrative interfaces- Console- Remote desktop- Secure shell (SSH)- Web interface

2.4 The key concepts of high availability for servers.

• Clustering- Active-active- Active-passive- Failover- Failback- Proper patching procedures- Heartbeat

• Fault tolerance- Server-level redundancy vs. component redundancy

• Redundant server network infrastructure- Load balancing- Software vs. hardware- Round robin- Most recently used (MRU)- Network interface card (NIC) teaming and redundancy - Failover- Link aggregation

2.5 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 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 The importance of asset management and documentation.

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

2.8 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 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

3.1 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 Concepts pertaining to identity and access management for server administration.

User accounts
• User groups
• Password policies- Length- Lockout- Enforcement

• Permissions and access controls- Role-based- Rule-based- Scope based- Segregation of duties- Delegation

• Auditing- User activity- Logins- Group memberships- Deletions

• Multifactor authentication (MFA)- Something you know- Something you have- Something you are

• Single sign-on (SSO)

3.4 Data security risks and mitigation strategies.

• Security risks- Hardware failure- Malware- Data corruption- Insider threats- Theft- Data loss prevention (DLP)- Unwanted duplication- Unwanted publication- Unwanted access methods- Backdoor- Social engineering- Breaches - Identification - Disclosure

• Mitigation strategies- Data monitoring- Log analysis- Security information and event management (SIEM)- Two-person integrity- Split encryption keys tokens- Separation of roles- Regulatory constraints - Governmental- Individually privileged information- Personally identifiable information (PII)- Payment Card Industry Data Security Standard (PCI DSS)- Legal considerations- Data retention - Subpoenas

3.5 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 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 The importance of backups and restores.

• Backup methods- Full- Synthetic full- Incremental- Differential- Archive- Open file- Snapshot

• Backup frequency

• Media rotation

• Backup media types- Tape- Cloud- Disk- Print

• File-level vs. system-state backup

• Restore methods- Overwrite- Side by side- Alternate location path

• Backup validation- Media integrity- Equipment - Regular testing intervals

• Media inventory before restoration

3.8 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 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 Troubleshoot common hardware failures.

• Common problems- Predictive failures- Memory errors and failures- System crash- Blue screen- Purple screen- Memory dump - Utilization- Power-on self-test (POST) errors- Random lockups- Kernel panic- Complementary metal-oxide- semiconductor (CMOS) battery failure- System lockups- Random crashes- Fault and device indication- Visual indicators- Light-emitting diode (LED)- Liquid crystal display (LCD)

panel readouts- Auditory or olfactory cues - POST codes- Misallocated virtual resources

• Causes of common problems- Technical- Power supply fault - Malfunctioning fans - Improperly seated heat sink - Improperly seated cards- Incompatibility of components - Cooling failures - Backplane failure - Firmware incompatibility - CPU or GPU overheating- Environmental - Dust - Humidity - Temperature

• Tools and techniques- Event logs- Firmware upgrades or downgrades- Hardware diagnostics- Compressed air- Electrostatic discharge (ESD) equipment- Reseating or replacing components and/or cables

4.3 Troubleshoot storage problems.

• Common problems- Boot errors- Sector block errors- Cache battery failure- Read/write errors- Failed drives- Page/swap/scratch file or partition- Partition errors- Slow file access- OS not found- Unsuccessful backup- Unable to mount the device- Drive not available- Cannot access logical drive- Data corruption- Slow I/O performance- Restore failure- Cache failure- Multiple drive failure

• Causes of common problems- Disk space utilization - Insufficient disk space- Misconfigured RAID- Media failure- Drive failure- Controller failure- Hot bus adapter (HBA) failure- Loose connectors- Cable problems- Misconfiguration- Corrupt boot sector- Corrupt filesystem table- Array rebuild- Improper disk partition- Bad sectors- Cache battery failure- Cache turned off- Insufficient space- Improper RAID configuration- Mismatched drives- Backplane failure

• Tools and techniques- Partitioning tools- Disk management- RAID and array management- System logs- Disk mounting commands- net use - mount- Monitoring tools- Visual inspections- Auditory inspections

4.4 Troubleshoot common OS and software problems.

• Common problems- Unable to log on- Unable to access resources- Unable to access files - System file corruption- End of life/end of support- Slow performance- Cannot write to system logs- Service failures- System or application hanging- Freezing- Patch update failure

• Causes of common problems- Incompatible drivers/modules- Improperly applied patches- Unstable drivers or software- Server not joined to domain- Clock skew- Memory leaks- Buffer overrun- Incompatibility- Insecure dependencies- Version management - Architecture- Update failures- Missing updates- Missing dependencies- Downstream failures due to updates- Inappropriate application- level permissions- Improper CPU affinity and priority

• OS and software tools and techniques- Patching - Upgrades - Downgrades- Package management- Recovery- Boot options- Safe mode- Single user mode- Reload OS - Snapshots- Proper privilege escalations- runas/Run As - sudo - su- Scheduled reboots- Software firewalls- Adding or removing ports - Zones- Clocks- Network time protocol (NTP)- System time- Services and processes - Starting - Stopping- Status identification - Dependencies- Configuration management- System center configuration manager (SCCM) - Puppet/Chef/Ansible- Group Policy Object (GPO)- Hardware compatibility list (HCL)

4.4 Troubleshoot common OS and software problems.

• Common problems- Unable to log on- Unable to access resources- Unable to access files - System file corruption- End of life/end of support- Slow performance- Cannot write to system logs- Service failures- System or application hanging- Freezing- Patch update failure

• Causes of common problems- Incompatible drivers/modules- Improperly applied patches- Unstable drivers or software- Server not joined to domain- Clock skew- Memory leaks- Buffer overrun- Incompatibility- Insecure dependencies- Version management - Architecture- Update failures- Missing updates- Missing dependencies- Downstream failures due to updates- Inappropriate application- level permissions- Improper CPU affinity and priority

• OS and software tools and techniques- Patching - Upgrades - Downgrades- Package management- Recovery- Boot options- Safe mode- Single user mode- Reload OS - Snapshots- Proper privilege escalations- runas/Run As - sudo - su

4.5 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 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)