CompTIA Server+ (2009 Edition) Certification Examination Objectives

DRAFT

INTRODUCTION

The CompTIA Server+ (2009 Edition) certification is an international vendor neutral credential. The Server+ exam is a validation of "foundation" level server skills and knowledge, and is used by organizations and IT professionals around the globe.

The skills and knowledge measured by this examination are derived from an industry-wide Job Task Analysis (JTA) and were validated through a global survey in Q4, 2008. The results of the survey were used to validate the content of the subject areas (domains) and exam objectives, as well as the overall domain weightings, ensuring the importance of one domain relative to another.

The CompTIA Server+ (2009 Edition) certification is targeted towards individuals with 18-24 months of IT experience. Although not a prerequisite, it is recommended that CompTIA Server+ candidates hold a CompTIA A+ certification.

This test will certify that the successful candidate has the knowledge and skills required to build, maintain, troubleshoot and support server hardware and software technologies. The successful candidate will be able to identify environmental issues; understand and comply with disaster recovery and physical / software security procedures; be familiar with industry terminology and concepts; understand server roles / specializations and interaction within the overall computing environment.

The table below lists the domains measured by this examination and the appropriate extent to which they are represented.

Domain	% of Examination
1.0 System Hardware	21%
2.0 Software	19%
3.0 Storage	14%
4.0 IT Environment	11%
5.0 Disaster Recovery	11%
6.0 Troubleshooting	24%
Total	**100%**

**Note: The lists of examples provided in bulleted format below each objective 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.

(A list of acronyms used in these Objectives appears at the end of this document.)

1.0 System Hardware

1.1 Differentiate between system board types, features, components and their purposes.

- Dip switches / jumpers
- Processor (single and multi)
- Bus types and bus speeds
- On board components
  - NICs
  - Video
  - Audio
  - USB
  - HID
  - Serial
  - Parallel
- Expansion slots
  - PCI
  - PCIe
  - PCIx
  - AGP
  - ISA
- BIOS
- Riser Card / backplane
- Storage connectors
  - SCSI
  - SATA
  - IDE
  - Floppy

1.2 Deploy different chassis types and the appropriate components

- Cooling
  - Fans
  - Water cooled
  - Passive
  - Active
  - Shroud
  - Ducts
  - Redundant cooling
  - Hot swappable
  - Ventilation
- Form Factor (tower, rack, blade)
  - Space utilization (U size, height, width, depth)
- Power
  - Connectors
  - Voltages
  - Phase
- Redundant power
- Shut off switches – chassis intrusion
- Power buttons
- Reset buttons
- Diagnostic LEDs
- Expansion bays

1.3 Differentiate between memory features / types and given a scenario select appropriate memory

- Memory pairing
- ECC vs. non ECC
- Registered vs. non-registered
- RAID and hot spares
- Types
    - DDR
    - Fully buffered DIMM
    - DDR2
    - SDRAM
    - DDR3
- Memory compatibility
    - Speed
    - Size
    - Pins
    - CAS latency
    - Timing
    - Vendor specific memory
- On board vs. riser card

1.4 Explain the importance of a Hardware Compatibility List (HCL)

- Vendor standards for hardware
- Memory and processor compatibility
- Expansion cards compatibility
- Virtualization requirements

1.5 Differentiate between processor features / types and given a scenario select the appropriate processor

- Multicore
- Multiprocessor
- Cache levels
- Stepping
- Speed
- VRMs
- Execute disable (XD) or not execute (NX)
- Hyperthreading
- VT or AMD-V
- AMD vs.Intel (non-compatible CPUs)
- Processor architecture (RISC, CISC)
- Vendor slot types
- 64bit vs. 32 bit
- Heat dissipation (heat sinks, fans, liquid cooling)

1.6 Given a scenario, install appropriate expansion cards into a server while taking fault tolerance into consideration.

- Manufacturer specific
    - Fax cards
    - PBX cards
    - Camera cards
    - VoIP
- HBAs

- NICs
- Video
- Audio
- Storage controller (SCSI, SATA, RAID)
    - SCSI low voltage / high voltage (LVD/HVD)
    - SCSI IDs
    - Cables and connectors
    - Active vs. passive termination
- Port expansion cards
    - USB
    - IEEE 1394
    - Serial
    - Parallel

1.7 Install, update and configure appropriate firmware.

- Driver / hardware compatibility
- Implications of a failed firmware upgrade (redundant BIOS)
- Follow manufacturer instructions and documentation

2.0 Software

2.1 Install, deploy, configure and update NOS (Windows / *nix).

- Installation methods (optical media, USB, network share, PXE)
    - Imaging – system cloning and deployment (Ghost, RIS/WDS, Altiris, virtualization templates)
- Bootloader
- File systems
    - FAT
    - FAT32
    - NTFS
    - VMFS
    - ZFS
    - EXT3
- Driver installation
    - Driver acquisition
    - Installation methods
    - Require media
- Configure NOS
    - Initial network
    - User
    - Device
    - Roles
    - OS environmental settings
    - Applications and tools
- Patch management

***2.2* Explain NOS security software and its features.**

- Software firewall
    - Port blocking
    - Application exception
    - ACL
- Malware protection software
    - Antivirus

    - Antispyware
- Basics of file level permissions vs. share permissions

2.3 Given a scenario, implement and administer NOS management features based on procedures and guidelines

- User management
    - Add and remove users
    - Setting permissions
    - Group memberships
    - Policies
    - Logon scripts
- Resource management
    - ACLs
    - Quotas
    - Shadow volumes
    - Disk management
    - Performance monitoring
    - Baselining
- Monitoring (tools and agents)
    - SNMP (MIBs)
    - WBEM (WMI)

2.4 Explain different server roles, their purpose and how they interact

- File and print server
- Database server
- Web server
- Messaging server
- DHCP server
- Directory services server
- DNS server
- Application server
    - Update server and proxy server
    - Filtering server
    - Monitoring server
    - Dedicated
    - Distributed
    - Peer to peer
- Remote access server
- Virtualized services
- NTP server
- Explain the different between a workstation, desktop and a server
- Server shut down and start up sequence (one server vs. multiple servers vs. attached components)

2.5 Summarize server virtualization concepts, features and considerations

- Resource utilization
- Configuration
- Interconnectivity
- Management server
- Reasons for virtualization
    - Cost benefits
    - Redundancy
    - Green initiative
    - Disaster recovery
    - Testing environment

- Ease of deployment

2.6 Describe common elements of networking essentials

- TCP/IP
  - Subnetting
  - DNS
  - DHCP
  - Classes
  - Gateways
  - Static vs. dynamic
  - IP stack
  - Ports
- Ethernet
  - Types
  - Speeds
  - Cables
- VPN
- VLAN
- DMZ

3.0 Storage

3.1 Describe RAID technologies and its features and benefits

- Hot spare
- Software vs. hardware
- Cache read/write levels (data loss potential)
- Performance benefits and tradeoffs

3.2 Given a scenario, select the appropriate RAID level

- 0, 1, 3, 5, 6, 10, 50
- Performance benefits and tradeoffs

3.3 Install and configure different internal storage technologies

- Hot swappable vs. non-hot swappable
- SCSI, Ultra SCSI, Ultra320 (termination), LUNs
- SAS, SATA
- Tape
- Optical
  - DVD
  - DVD-R
  - CD-ROM
  - CD-R
  - CD-RW
  - Blu-Ray
- Flash
- Floppy (USB)
- Controller (firmware levels)
- Hard drive (firmware, JBOD)

3.4 Summarize the purpose of external storage technologies

- Network attached storage
- Storage area network
- Tape library

- WORM
- Optical jukebox
- Transport media
    - iSCSI
    - SATA
    - SAS
    - SCSI
    - Fiber Channel

4.0 IT Environment

4.1 Write, utilize and maintain documentation, diagrams and procedures

- Follow pre-installation plan when building or upgrading servers
- Labeling
- Diagram server racks and environment topologies
- Hardware and software upgrade, installation, configuration , server role and repair logs
- Document server baseline (before and after service)
- Original hardware configuration, service tags, asset management and warranty
- Vendor specific documentation
    - Reference proper manuals
    - Websites
    - Support channels (list of vendors)

4.2 Given a scenario, explain the purpose of the following industry best practices

- Follow vendor specific server best practices
    - Documentation
    - Tools
    - Websites
- Explore ramifications before implementing change – determine organizational impact
- Communicate with stakeholders before taking action and upon completion of action
- Comply with all local laws / regulations, industry and corporate regulations
- Purpose of Service Level Agreement (SLAs)
- Follow change control procedures
- Equipment disposal

4.3 Determine an appropriate physical environment for the server location

- Check for adequate and dedicated power, proper amperage and voltage
    - UPS systems (check load, document service, periodic testing)
    - UPS specifications (run time, max load, bypass procedures, server communication and shut down, proper monitoring)
- Server cooling considerations – HVAC
    - Adequate cooling in room
    - Adequate cooling in server rack
    - Temperature and humidity monitors

4.4 Implement and configure different methods of server access

- KVM (local and IP based)
- Direct connect
- Remote management

    - Remote control
    - Administration
    - Software deployment
    - Dedicated management port

4.5 Given a scenario, classify physical security measures for a server location

- Physical server security
    - Locked doors
    - Rack doors
    - CCTV
    - Mantraps
    - Security personnel
- Access control devices (RFID, keypads, pinpads)
    - Biometric devices (fingerprint scanner, retina)
- Security procedures
    - Limited access
    - Access logs
    - Limited hours
- Defense in-depth – multiple layers of defense
- Reasons for physical security
    - Theft
    - Data loss
    - Hacking
- Secure documentation related to servers
    - Passwords
    - System configurations
    - Logs

5.0 Disaster Recovery

5.1 Compare and contrast backup and restoration methodologies, media types and concepts

- Methodologies (full, incremental, differential)
    - Snapshot
    - Copy
    - Bare metal
    - Open file
    - Databases
    - Data vs. OS restore
    - Rotation and retention (grandfather, father and son)
- Media types
    - Tape
    - Disk
    - WORM
    - Optical
    - Flash
- Backup security and off-site storage
- Importance of testing the backup and restoration process

5.2 Given a scenario, compare and contrast the different types of replication methods

- Disk to disk
- Server to server
    - Clustering

    - Active/active
    - Active/passive
- Site to site
- Site types
    - Cold site
    - Hot site
    - Warm site
    - Distance requirements

5.3 Explain data retention and destruction concepts

- Awareness of potential legal requirements
- Awareness of potential company policy requirements
- Differentiate between archiving and backup

5.4 Given a scenario, carry out the following basic steps of a disaster recovery plan

- Disaster recovery testing process
- Follow emergency procedures (people first)
- Use appropriate fire suppressants
- Follow escalation procedures for emergencies
- Classification of systems (prioritization during recovery)

6.0 Troubleshooting

6.1 Explain troubleshooting theory and methodologies

- 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
- Establish a theory of probable cause (question the obvious)
    - Determine whether there is a common element of symptom causing multiple problems
- Test the theory to determine cause
    - Once theory is confirmed determine next steps to resolve problem
    - If theory is not confirmed re-establish new theory or escalate
- Establish a plan of action to resolve the problem and notify impacted users
- 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
- Verify full system functionality and if applicable implement preventative measures
- Performa a root cause analysis
- Document findings, actions and outcomes throughout the process

6.2 Given a scenario, effectively troubleshoot hardware problems, selecting the appropriate tools and methods

- 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
- Causes of common problems
    - Third party components or incompatible components
    - Incompatible or incorrect BIOS
    - Cooling failure
    - Mismatched components
    - Backplane failure
- Environmental issues
    - Dust
    - Humidity
    - Temperature
    - Power surge **/** failure
- Hardware tools
    - Power supply tester (multimeter)
    - System board tester
    - Compressed air
    - ESD equipment

6.3 Given a scenario, effectively troubleshoot software problems, selecting the appropriate tools and methods

- Common problems
    - User unable to logon
    - 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
- Cause of common problems
    - Malware
    - Unauthorized software
    - Software firewall
    - User Account Control (UAC/SUDO)
    - Improper permissions
    - Corrupted files
    - Lack of hard drive space
    - Lack of system resources
    - Virtual memory (misconfigured, corrupt)
    - Fragmentation
    - Encryption
    - Print server drivers/services

    - Print spooler
- Software tools
    - System logs
    - Monitoring tools (resource monitor, performance monitor)
    - Defragmentation tools

6.4 Given a scenario, effectively diagnose network problems, selecting the appropriate tools and methods

- Common problems
    - Internet connectivity failure
    - Email failure
    - Resource unavailable
    - DHCP server mis-configured
    - Non-functional or unreachable
    - Destination host unreachable
    - Unknown host
    - Default gateway mis-configured
    - Failure of service provider
    - Can reach by IP not by host name
- Causes of common problems
    - Improper IP configuration
    - VLAN configuration
    - Port security
    - Improper subnetting
    - Component failure
    - Incorrect OS route tables
    - Bad cables
    - Firewall (mis-configuration, hardware failure, software failure)
    - Mis-configured NIC, routing / switch issues
    - DNS and/or DHCP failure
    - Mis-configured hosts file
- Networking tools
    - ping
    - tracert / traceroute
    - ipconfig / ifconfig
    - nslookup
    - net use / mount
    - route
    - nbstat
    - netstat

6.5 Given a scenario, effectively troubleshoot storage problems, selecting the appropriate tools and methods

- 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
- Causes of common problems
    - Media failure
    - Drive failure
    - Controller failure
    - HBA failure
    - Loose connectors
    - Cable problems
    - Mis-configuration
    - Improper termination
    - Corrupt boot sector
    - Corrupt file system table
    - Array rebuild
    - Improper disk partition
    - Bad sectors
    - Cache battery failure
    - Cache turned off
    - Insufficient space
    - Improper RAID configuration
    - Mis-matched drives
    - Backplane failure
- Storage tools
    - Partitioning tools
    - Disk management
    - RAID array management
    - Array management
    - System logs
    - Net use / mount command
    - Monitoring tools

SERVER+ ACRONYMS

*nix	Unix/Linux/Solaris/OS X/BSD
AD	Active Directory
AGP	Advanced Graphics Port
AMD-V	AMD Virtualization
BIOS	Basic Input/Output System
BSOD	Blue Screen of Death
CPU	Central Processing Unit
CRU	Customer Replaceable Unit
DC	Domain Controller
DHCP	Dynamic Host Control Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Service
DSRM	Directory Services Restore Mode
EISA	Extended Industry Standard Architecture
FAT	File Allocation Table
FRU	Field Replaceable Unit
FTP	File Transfer Protocol
HBA	Host Bus Adapter
HCL	Hardware Compatibility List
HID	Human Interface Device
HTTP	Hyper Text Transport Protocol
HTTPS	Secure Hyper Text Transport Protocol
HVAC	Heating, Ventilating and Air Conditioning
IMAP4	Internet Mail Access Protocol
ISA	Industry Standard Architecture
iSCSI	Internetworking Small Computer Serial Interface
JBOD	Just a bunch of disks
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LKGC	Last Known Good Configuration
LUN	Logical Unit Number
NOS	Network Operating System
NTFS	New Technology File System
NTP	Network Time Protocol
NX	No Execute
OS	Operating System
OSPF	Open Shortest Path First
PCI	Peripheral Component Interconnect
POP3	Post Office Protocol

RAID	Redundant Array of Inexpensive/Integrated Disks/Drives
RAM	Random Access Memory
SAS	Serial Attached SCSI
SATA	Serial ATA
SCSI	Small Computer Serial Interface
SLA	Service Level Agreement
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMFS	VMWare File System
VoIP	Voice over IP
VPN	Virtual Private Network
VT	Virtualization Technology
WBEM	Web-based Enterprise Management
WMI	Windows Management Instrumentation
WORM	Write Once Read Many
XD	Execute Disable