This Cram Sheet contains the distilled, key facts about the CompTIA Server+ exam. Review this information immediately before entering the test room, paying special attention to those areas in which you feel you need the most review. Remember, you can transfer any of these facts that you've crammed into your short-term memory onto a blank piece of paper before beginning the exam.

Server Environment

1. Temperature-The temperature in a server will be approximately 20 to 30 degrees (Fahrenheit) higher than the temperature in the room. Room temperature above 80 and server temperature above 110 can cause damage.
2. Electricity-It is essential that proper electricity, including battery backup, is provided in a server room.
3. Humidity-Humidity above 20 to 30 percent could cause short circuits, and below this amount could cause circuit boards to become brittle.

Software/Firmware Installation and Upgrade

4. BIOS-Upgrading or flashing the BIOS requires a boot floppy disk that can usually be downloaded from the customer support link on the particular manufacturer's Web site. Once the floppy is booted, it will automatically run the BIOS upgrade process. A reboot thereafter is necessary.
5. SNMP/RMON-SNMP and RMON alerts might be in place to indicate network utilization, processor utilization, and so on. Network utilization lower than 60 percent is not a concern. SNMP and RMON traps can also be changed to report different thresholds, and the management application can be changed to notify you at different ranges.

Hardware Upgrade and Installation

6. Memory
   * Server motherboards have a limit on how much RAM they can support and the maximum supported memory in a single SIMM.
   * Many servers have problems with different SIMMs being on the same machine or on the same memory bank. Some systems require that the same memory speeds be on the system; others require that identical capacity SIMMs be in place, and still others require that everything be identical including the manufacturer.
7. CPU-Adding a CPU will require a BIOS upgrade.
8. SCSI
   * When anything goes wrong, check termination and LUN.
   * HVD is not compatible with LVD or SE.
   * LVD and SE devices are compatible with each other but will run at the slower SE bus speeds.
   * 8-bit (SCSI, Fast, Ultra, and Ultra2) SCSI internal devices are male; cables are female.
   * 16-bit (Wide, Fast Wide, Wide Ultra, Wide Ultra2, Ultra3, Ultra160/160+/320) internal devices are female; cables are male.
   * External devices are female; connectors are male.
   * Rule of thumb-50-pin connectors go with 8-bit SCSI standards, and 68-pin connectors are for 16-bit SCSI. Table 1 lists the SCSI standards.
9. RAID
   * Software-based RAID relies on the CPU for processing the RAID algorithms. If server performance decreases immediately after a RAID installation, it is due to the software-based RAID. The solution is to either change to hardware-based RAID or upgrade the CPU.
   * Hardware-based RAID enables features such as hot swapping, which allows a replacement drive to be installed without taking down the server.
10. I/O bus-ISA is slower than MCI, which is proprietary. EISA was developed to compete with MCI and is backward compatible. EISA device installation requires that the EISA CONFIG application be run to properly identify and configure the server. PCI came along and basically replaced all previous bus types because it is faster and has plug-and-play features, but it is not backward compatible with anything. AGP is not really an I/O bus, but a port.
11. External connections-SCSI is the fastest standard. IEEE 1394 (Firewire) is second fastest.

Networking and Connectivity

12. Cabling
    * Crossover cables are used to connect two servers to each other and two hubs to each other without a crossover port. On one side of the cable, wires are labeled 1, 2, 3, 4, 5, 6, 7, 8. On the other side of the cable, wires are crossed over to be 3, 6, 1, 4, 5, 2, 7, 8.
    * Straight cables are used to connect servers to hubs/switches and hubs to other hubs or switches, providing the connection is through a crossover port.
14. Connectivity-Check connectivity if someone is unable to log in, connect, or access another system or the Web.
    * Use Windows Explorer (if applicable) to ensure that the computer is accessible.
    * Use the PING 127.0.0.1 command to first check that the IP protocol is bound to the local computer network card.
    * PING the address of the server in question. Also use TRACERT to see if there are any breaks in communication between you and the server in question.
    * Use IPCONFIG/IFCONFIG to check your current TCP/IP configuration and also to reconfigure DHCP client information.
15. Network Operating Systems
    * Novell NetWare is strictly an NOS that configures hard disks as volumes and still uses DOS as its base operating system. The base volume is called "sys." NetWare services/daemons are called NetWare Loadable Modules (NLMs). Server shutdown occurs using the command **down** followed by **exit**, which will exit to a DOS prompt. Typing **server** reinitializes the server.
    * Windows NT/2000 is both an OS and an NOS that uses hard disks formatted with the NTFS format but also supports FAT32 formats. Daemons/NLMs for Windows NT/2000 are called services. Server shutdown occurs by either pressing Ctrl+Alt+Del followed by clicking the Shutdown button or by selecting Start menu | Shutdown and then choosing Shutdown or Restart.
    * Unix and Linux are both OSs and NOSs that use hard disks formatted with the NIS or NFS file system. Services or NLMs for Unix and Linux are called daemons. Server shutdown occurs by using the command **shutdown now -g -0**.

Disaster Recovery and Fault Tolerance

16. Disaster Protection
    * Data Loss
      * RAID 1 offers mirroring (one drive controller) or duplexing (two drive controllers), and 50 percent of the overall disk space is available for data storage. RAID 5 offers striping with parity, and the available disk space is one less than the number of drives installed on the stripe set.
      * Tape backup and rotation schemes can include a GFS rotation method. A full backup occurs once a month (grandfather), a full backup occurs once a week (father), and an incremental or differential backup occurs once a day. Remember that tape backups can also be used for archiving for long periods of time.
    * Fire/flood/complete destruction-Protection from fire is provided when storing tape backups in a fireproof safe on the

premises. Protection from flood and complete destruction requires offsite backup storage.

* Power loss requires a UPS unit. UPSs can be installed with management software that can perform remote notification and automatic system shutdown.

17. Data Center Destruction

* Hot sites are available for use within 48 hours. Most, if not all, equipment is onsite.
* Cold sites are available for use within a few weeks. None of the necessary equipment is onsite, and building, structure, or office modifications may be necessary.
* Offsite tape storage is required to recover from any full destruction situation.

18. Fault Tolerance

* Technologies
  * Hot swap occurs when a failed component can be replaced without taking down the server.
  * Hot plug is a feature whereby a spare component is installed and automatically comes online when an identical component fails. This occurs without taking down the server.
* Hardware
  * Dual PCI buses are used to help prevent a single bus from becoming flooded with traffic. The second bus is usually used for RAID controller cards.
  * Dual network cards are used to reduce problems with a single NIC, cable, or hub/switch port.
  * Dual CPUs are primarily used for additional power; however, failover procedures can allow a system to boot from a different CPU if the first one fails. For this reason, a BIOS upgrade is necessary when installing a second CPU.
  * Fault-tolerant cooling fans and power supplies are simply hot-swappable devices found in servers.
  * RAID 0 is not fault tolerant, but it is fast and has 100 percent available disk space.
  * RAID 1 offers mirroring or duplexing, has 50 percent available disk space, is slower than RAID 0,and is also slower than a single drive.
  * RAID 5 offers striping with parity, has available disk space equal to the capacity of the disks minus one, and is faster than RAID 1 but slower than RAID 0.
  * Hardware-based RAID array configuration supports hot swapping and hot plugging and is configured using a RAID BIOS. Changing the order in which the hard drives are configured in an array requires reconfiguration, during which all data will be lost. Hardware-based RAID has a separate processor and is not CPU intensive.
  * Software-based RAID does not support hot swapping or hot plugging and is configured using the NOS or supported application. Drive replacement occurs by taking down the server. Software-based RAID is CPU intensive.

Troubleshooting

19. Baselines should cover pertinent server usage information over a period of several days or a week. The same data should be gathered again and compared with the baselines during the troubleshooting process.
  * High memory utilization can indicate bad or failing RAM.
  * High CPU utilization may indicate software-based RAID or a failing CPU.
  * High pages/second can indicate that there is not enough RAM or that the RAM is failing.
  * High hard disk utilization might point to insufficient drive space, a failing hard drive, or a paging problem (for paging problems, refer to the previous bulleted item).
20. Services and daemons are primarily software issues, but because services and daemons work closely with drivers, they can be hardware related. When a service or daemon fails, restart the daemon. If it fails again, reboot the server. If it fails yet again, disable or remove other services by using a process of elimination.
21. Antivirus software can be configured to automatically update from the Web. Communications for this usually occur via FTP. If the update fails, check to ensure that the FTP site is available, and also check to ensure that outbound communications are intact.