INTRODUCTION

The CompTIA Server+ certification is an international vendor neutral credential. The CompTIA 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+ 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.

<table>
<thead>
<tr>
<th>Domain</th>
<th>% of Examination</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 System Hardware</td>
<td>21%</td>
</tr>
<tr>
<td>2.0 Software</td>
<td>19%</td>
</tr>
<tr>
<td>3.0 Storage</td>
<td>14%</td>
</tr>
<tr>
<td>4.0 IT Environment</td>
<td>11%</td>
</tr>
<tr>
<td>5.0 Disaster Recovery</td>
<td>11%</td>
</tr>
<tr>
<td>6.0 Troubleshooting</td>
<td>24%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>
CompTIA Authorized Materials Use Policy

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse or condone utilizing any content provided by unauthorized third-party training sites, aka 'brain dumps'. Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA’s exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the CompTIA Certification Exam Policies webpage:

http://certification.comptia.org/Training/testingcenters/policies.aspx

Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the CompTIA Candidate Agreement (http://certification.comptia.org/Training/testingcenters/policies/agreement.aspx) at the time of exam delivery.

If a candidate has a question as to whether study materials are considered unauthorized (aka brain dumps), he/she should perform a search using CertGuard's engine, found here:

http://www.certguard.com/search.asp

Or verify against this list:

**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.

**CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.**

(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)
- Hyper-Threading
- 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)
  o SCSI low voltage / high voltage (LVD/HVD)
  o SCSI IDs
  o Cables and connectors
  o Active vs. passive termination
• Port expansion cards
  o USB
  o IEEE 1394
  o Serial
  o 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)
  o Imaging – system cloning and deployment (Ghost, RIS/WDS, Altiris, virtualization templates)
• Bootloader
• File systems
  o FAT
  o FAT32
  o NTFS
  o VMFS
  o ZFS
  o EXT3
• Driver installation
  o Driver acquisition
  o Installation methods
  o Require media
• Configure NOS
  o Initial network
  o User
  o Device
  o Roles
  o OS environmental settings
  o Applications and tools
• Patch management

2.2 Explain NOS security software and its features.
• Software firewall
  o Port blocking
  o Application exception
  o ACL
• Malware protection software
  o Antivirus
  o 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
  o Add and remove users
  o Setting permissions
  o Group memberships
  o Policies
  o Logon scripts
• Resource management
  o ACLs
  o Quotas
  o Shadow volumes
  o Disk management
  o Performance monitoring
  o Baselining
• Monitoring (tools and agents)
  o SNMP (MIBs)
  o 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
  o Update server and proxy server
  o Filtering server
  o Monitoring server
  o Dedicated
  o Distributed
  o 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
  o Cost benefits
  o Redundancy
  o Green initiative
  o Disaster recovery
  o Testing environment
  o Ease of deployment
2.6 Describe common elements of networking essentials
   • TCP/IP
     o Subnetting
     o DNS
     o DHCP
     o Classes
     o Gateways
     o Static vs. dynamic
     o IP stack
     o Ports
     o Teaming/Link Aggregation
   • Ethernet
     o Types
     o Speeds
     o 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
     o DVD
     o DVD-R
     o CD-ROM
     o CD-R
     o CD-RW
     o 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
  - Fibre 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
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)
  - 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, selective)
  - 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/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
- Perform 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
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
  - nbtstat
  - 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
- 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
ACL  Access Control List
AD  Active Directory
AGP  Accelerated Graphics Port
AIT  Advanced Intelligent Tape
AMD-V  AMD Virtualization
ATX  Advanced Technology Extended
BBWC  Battery-Backed Write Cache
BIOS  Basic Input/Output System
BSOD  Blue Screen of Death
BTX  Balanced Technology Extended
CAS  Column Address Strobe
CIDR  Classless Inter-Domain Routing
CLI  Command Line Interpreter
CPU  Central Processing Unit
CRT  Cathode Ray Tube (Monitor)
CRU  Customer Replaceable Unit
CUPS  Common Unix Printing System
DAS  Direct Attached Storage
DAT  Digital Audio Tape
DDoS  Distributed Denial of Service
DC  Domain Controller
DDR  Double Data Rate
DDR2  Double Data Rate2
DDR3  Double Data Rate3
DHCP  Dynamic Host Configuration Protocol
DLT  Digital Linear Tape
DMA  Direct Memory Access
DMZ  Demilitarized Zone
DNS  Domain Name Service
DSRM  Directory Services Restore Mode
DTX  Discontinuous Transmission
EDO  Extended Data Out
EIDE  Enhanced Integrated Drive Electronics
EISA  Extended Industry Standard Architecture
ESD  Electrostatic Discharge
FAT  File Allocation Table
FQDN  Fully Qualified Domain Name
FRU  Field Replaceable Unit
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GFS</td>
<td>Grandfather Father Son</td>
</tr>
<tr>
<td>GPU</td>
<td>Graphics Processing Unit</td>
</tr>
<tr>
<td>HBA</td>
<td>Host Bus Adapter</td>
</tr>
<tr>
<td>HCL</td>
<td>Hardware Compatibility List</td>
</tr>
<tr>
<td>HID</td>
<td>Human Interface Device</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hyper Text Transport Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Secure Hyper Text Transport Protocol</td>
</tr>
<tr>
<td>HVAC</td>
<td>Heating, Ventilating and Air Conditioning</td>
</tr>
<tr>
<td>HVD</td>
<td>High Voltage Differential</td>
</tr>
<tr>
<td>IIS</td>
<td>Internet Information Services</td>
</tr>
<tr>
<td>IMAP4</td>
<td>Internet Mail Access Protocol</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPv6</td>
<td>Internet Protocol Version 6</td>
</tr>
<tr>
<td>IPMI</td>
<td>Intelligent Platform Management Interface</td>
</tr>
<tr>
<td>ISA</td>
<td>Industry Standard Architecture</td>
</tr>
<tr>
<td>iSCSI</td>
<td>Internetworking Small Computer System Interface</td>
</tr>
<tr>
<td>JBOD</td>
<td>Just a bunch of disks</td>
</tr>
<tr>
<td>KVM</td>
<td>Keyboard-Video-Mouse</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>LKGC</td>
<td>Last Known Good Configuration</td>
</tr>
<tr>
<td>LOM</td>
<td>Lights Out Management</td>
</tr>
<tr>
<td>LTO</td>
<td>Linear Tape-Open</td>
</tr>
<tr>
<td>LUN</td>
<td>Logical Unit Number</td>
</tr>
<tr>
<td>LVD</td>
<td>Low Voltage Differential</td>
</tr>
<tr>
<td>MIB</td>
<td>Management Information Base</td>
</tr>
<tr>
<td>microBTX</td>
<td>Micro Balanced Technology Extended</td>
</tr>
<tr>
<td>miniATX</td>
<td>Micro Advanced Technology Extended</td>
</tr>
<tr>
<td>MMC</td>
<td>Microsoft Management Console</td>
</tr>
<tr>
<td>NAS</td>
<td>Network Attached Storage</td>
</tr>
<tr>
<td>NLB</td>
<td>Network Load Balancing</td>
</tr>
<tr>
<td>NLX</td>
<td>New Low Profile Extended</td>
</tr>
<tr>
<td>NOS</td>
<td>Network Operating System</td>
</tr>
<tr>
<td>NTFS</td>
<td>New Technology File System</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>NX</td>
<td>No Execute</td>
</tr>
<tr>
<td>OEM</td>
<td>Original Equipment Manufacturer</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First</td>
</tr>
<tr>
<td>OTDR</td>
<td>Optical Time Domain Reflectometer</td>
</tr>
<tr>
<td>PATA</td>
<td>Parallel Advanced Technology Attachment</td>
</tr>
<tr>
<td>PBX</td>
<td>Private Branch Exchange</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>PCI</td>
<td>Peripheral Component Interconnect</td>
</tr>
<tr>
<td>POP3</td>
<td>Post Office Protocol (version 3)</td>
</tr>
<tr>
<td>PXE</td>
<td>Preboot Execution Environment</td>
</tr>
<tr>
<td>RAID</td>
<td>Redundant Array of Inexpensive/Integrated Disks/Drives</td>
</tr>
<tr>
<td>RAM</td>
<td>Random Access Memory</td>
</tr>
<tr>
<td>RAS</td>
<td>Remote Access Server</td>
</tr>
<tr>
<td>RDP</td>
<td>Remote Desktop Protocol</td>
</tr>
<tr>
<td>RIS</td>
<td>Remote Installation Service</td>
</tr>
<tr>
<td>SAN</td>
<td>Storage Area Network</td>
</tr>
<tr>
<td>SAS</td>
<td>Serial Attached SCSI</td>
</tr>
<tr>
<td>SATA</td>
<td>Serial ATA</td>
</tr>
<tr>
<td>SCSI</td>
<td>Small Computer System Interface</td>
</tr>
<tr>
<td>SDRAM</td>
<td>Synchronous Dynamic Random Access Memory</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SMP</td>
<td>Symmetric Multiprocessing</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transport Protocol</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol / Internet Protocol</td>
</tr>
<tr>
<td>TFTP</td>
<td>Trivial File Transfer Protocol</td>
</tr>
<tr>
<td>TDR</td>
<td>Time Domain Reflectometer</td>
</tr>
<tr>
<td>UAC</td>
<td>User Account Control</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UID</td>
<td>Unit Identification</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>VMFS</td>
<td>VMWare File System</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over IP</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>VRM</td>
<td>Voltage Regulator Module</td>
</tr>
<tr>
<td>VSS</td>
<td>Volume Shadow Service</td>
</tr>
<tr>
<td>VT</td>
<td>Virtualization Technology</td>
</tr>
<tr>
<td>WBEM</td>
<td>Web-based Enterprise Management</td>
</tr>
<tr>
<td>WDS</td>
<td>Windows Deployment Services</td>
</tr>
<tr>
<td>WMI</td>
<td>Windows Management Instrumentation</td>
</tr>
<tr>
<td>WORM</td>
<td>Write Once Read Many</td>
</tr>
<tr>
<td>WSUS</td>
<td>Windows Software Update Services</td>
</tr>
<tr>
<td>XD</td>
<td>Execute Disable</td>
</tr>
<tr>
<td>ZFS</td>
<td>Zettabyte File System</td>
</tr>
</tbody>
</table>