

CompTIA Server+ Certification

*Complete coverage of all CompTIA Server+
certification objectives*

Ron Gilster



www.bpbonline.com

First Edition 2024

Copyright © BPB Publications, India

ISBN: 978-93-55513-861

All Rights Reserved. No part of this publication may be reproduced, distributed or transmitted in any form or by any means or stored in a database or retrieval system, without the prior written permission of the publisher with the exception to the program listings which may be entered, stored and executed in a computer system, but they can not be reproduced by the means of publication, photocopy, recording, or by any electronic and mechanical means.

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true to correct and the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

To View Complete
BPB Publications Catalogue
Scan the QR Code:



www.bpbonline.com

Kup książkę

Dedicated to

*My wife **Connie**
whose prayers, love and
support have been constant*

About the Author

Ron Gilster has written over 50 books on a variety of topics in the areas of IT career certifications, programming, computer technology, and a few in finance, real estate, and business. His commitment to his readers has always been a desire for their success.

Ron's career has included a range of IT-related positions that range from machine operator to programmer, to instructor, and to senior executive. He has worked in higher education, consulting, manufacturing, software development, and telecommunications.

About the Reviewer

Simone Bertulli is a cyber-security professional, currently holding a senior position at the Cyber Defense Center of an important Italian company.

He has more than 15 years of experience in the IT field and with expertise in Enterprise-class infrastructure technologies, where he obtained the CompTIA Server+, CompTIA Cloud Essentials, CompTIA Cloud+, CompTIA Storage+, CompTIA Linux+ and the LPIC-3 Virtualization & High Availability certifications.

He is a passionate supporter of Open Source, he actively contributes to the Community, writing on the Linux Professional Institute blog and holding tech talks always on FOSS themes, both on technical fields and on professional training.

Acknowledgement

I want to express my deepest gratitude to my wife Connie for her unwavering support and encouragement throughout the creation of this book.

I am very grateful to BPB Publications for this opportunity and for their guidance and expertise in bringing this book to fruition. I would especially like to express my appreciation for the hard work of Bertulli Simone Davide, the technical reviewer, and the BPB editors, whose assistance and guidance were valuable to produce this book's overall quality.

Preface

Although the CompTIA Server+ Certification may not be as well-known as other CompTIA certifications, such as A+, Network+, and Security+, and a few others, it does verify that its holder has the knowledge and understanding of the configurations, operations, and security of network servers and their components. The Server+ certification is intended for IT professionals with two- to four-years of experience working with network servers and computer networks.

CompTIA Server+ is a vendor-neutral certification that is at the same level as vendor-specific certifications, such as the Microsoft MCSA Server Administrator and Cisco Systems'CCNA Data Center. Unlike the Microsoft and Cisco certifications, CompTIA Server+ covers a broader base of server and networking fundamental principles, rather than a specific product line.

The Server+ exam verifies knowledge and understanding in four specific areas: server hardware installation and management, server administration, security and disaster recovery, and troubleshooting.

This book provides information and detail for each of the specific areas identified in the Server+ certification examination's objectives. The material presented is specific to each of the objective items areas to provide the reader with the knowledge and understanding it requires. This book provides in-depth explanations and discussions for all the concepts measured by the exam. It is written at a level that prepares both the well-experienced and the less-experienced IT professionals to prepare for the successful completion of the Server+ certification exam with a qualifying score.

The material presented in each of the chapters is outlined in the following summaries:

Chapter 1: Physical Hardware – This chapter focuses on the server's internal and external components, racking, cabling, and support hardware. The hardware generally discussed is most commonly associated with larger networks and data centers, but the systems found in smaller networks is also addressed. The specific areas covered in this chapter are: racking systems, power cabling, network cabling, server chassis types, and server components.

Chapter 2: Data Storage – This chapter focuses on various technologies used in data storage devices, including hard disk drives, RAID levels and types, capacity planning, hard drive media types, interface types, and shared storage.

Chapter 3: Server Hardware Maintenance – This chapter reviews the administration, management, and preventive maintenance of local and remote server hardware processes and procedures, including out-of-band management, local hardware administration, drive maintenance, hot-swappable hardware, firmware upgrades, and BIOS/UEFI.

Chapter 4: Server Operating Systems – This chapter reviews the administration, management, and preventive maintenance of local and remote server hardware processes and procedures, including minimum hardware requirements, operating system installations, installation types, partition and volume types, and file system types

Chapter 5: Network Infrastructure Services – This chapter reviews the administration, management, and preventive maintenance of local and remote server hardware processes and procedures, including IP configuration, addressing protocols, firewalls, static vs. dynamic routing, and MAC addressing.

Chapter 6: Configure Network Servers – This chapter reviews the administration, management, and preventive maintenance of local and remote server hardware processes and procedures, including server roles and requirements, storage management, server monitoring, data migration and transfer, and administrative interfaces.

Chapter 7: High Availability – This chapter discusses the technologies and methods associated with high availability, fault tolerance, clustering, load balancing, and redundant server network infrastructures.

Chapter 8: Virtualization – This chapter discusses the fundamentals of virtualization and its use in a networking environment, including virtualization, host vs. guest virtualization, resource allocation and provisioning, VM testing, and cloud models.

Chapter 9: Scripting – This chapter looks at how scripts are used in system and network administration. Its specific topics include scripting in server administration, script types, basic scripting constructs, scripting terminology, basic data types, Windows and Linux environmental variables, and script commenting.

Chapter 10: Asset Management – This chapter looks at the process of asset management, including documentation management, document availability, and the policies and procedures of asset management.

Chapter 11: Licensing – This chapter looks at the various types of software versions along with the conditions and rights a software provider grants its users, including software licensing, licensing agreements, licensing models, and version compatibility.

Chapter 12: Data Security – This chapter looks at the methods, processes, and concepts of data security, including encryption, data retention policies, data storage, data protection, and business impacts.

Chapter 13: Physical Security – This chapter looks at the physical security approaches, devices, and environmental controls that an organization can install to protect its systems, including access controls, architectural security reinforcements, authentication factors, and environment controls.

Chapter 14: Access Management – Access management is primarily an information security, IT and data governance process used to grant access to valid users and prohibit invalid users. This chapter covers user accounts, access controls, permissions, auditing, and single sign-on.

Chapter 15: Risk and Mitigation – This chapter discusses the risks to which servers are exposed, how those risks may be mitigated, and the regulatory and legal constraints that must be incorporated into an organization's security program, including security information and event management (SIEM).

Chapter 16: Server Hardening and Decommissioning – This chapter deals with keeping the operating system and applications up-to-date with fixes, updates, patches and the processes required to secure a network server, including hardening, patch management, change management, server decommissioning, media destruction, media retention requirements, and electronics recycling.

Chapter 17: Backup and Restore – This chapter looks at various aspects and practices of a backup and restore policy, including backup and recovery methods, restore methods, and backup validation.

Chapter 18: Disaster Recovery – This chapter discusses the elements and actions that may be a part of a disaster recovery plan, including disaster recovery planning, recovery sites, replication, testing, failovers and failbacks, and testing.

Chapter 19: Troubleshooting Methods – This chapter reviews the methods recommended for use when troubleshooting a failure or fault in any general hardware, software, network, storage device, and security policies or devices. This chapter covers the standard troubleshooting steps and the documentation of findings, actions, and outcomes.

Chapter 20: Hardware Issues – This chapter looks at the problems that can occur on server hardware, including memory issues, causes of common problems, and tools and techniques.

Chapter 21: Storage Issues – This chapter looks at data storage devices, their issues and causes, and the processes used to detect them, including common storage device problems, and the causes of common storage problems.

Chapter 22: Operating System and Software Issues – This chapter reviews common software problems, their causes, and some of the tools and utilities used to troubleshoot them.

Chapter 23: Software Tools and Techniques – This chapter looks at the tools and techniques available to resolve and fix problems and issues associated with a network server.

Chapter 24: Network Connectivity Issues – This chapter identifies the common problems, issues and their causes that occur on a computer network.

Chapter 25: Network Tools and Techniques – This chapter identifies the network operating system utilities and tools that are commonly a part of the troubleshooting process.

Chapter 26: Troubleshooting Security Issues – This chapter discusses the common data security concerns associated with network servers and the security tools used to diagnose and remedy any issues found.

Appendix A: CompTIA Server+ Certification Exam: Practice Test 1

Appendix B: CompTIA Server+ Certification Exam: Practice Test 2

Appendix C: CompTIA Server+® Acronyms

Appendix D: Key Terms/Concepts

Appendix E: Answers to Practice Test 1

Appendix F: Answers to Practice Test 2

Coloured Images

Please follow the link to download the
Coloured Images of the book:

<https://rebrand.ly/xtukgt4>

We have code bundles from our rich catalogue of books and videos available at **<https://github.com/bpbpublications>**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Did you know that BPB offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.bpbonline.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at :

business@bpbonline.com for more details.

At **www.bpbonline.com**, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on BPB books and eBooks.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

<https://discord.bpbonline.com>



Table of Contents

Part - 1: Server Hardware Installation and Management	1
1. Physical Hardware	3
Introduction.....	3
Structure.....	4
Objective	4
Racking systems	4
<i>Rack dimensions</i>	<i>5</i>
<i>Rack layout</i>	<i>5</i>
<i>Cooling management.....</i>	<i>6</i>
<i>Safety</i>	<i>6</i>
<i>Power Distribution Unit.....</i>	<i>7</i>
<i>Keyboard-Video-Mouse</i>	<i>7</i>
Power cabling.....	8
Redundant Power.....	8
Uninterrupted Power Supply	9
Separate circuits.....	9
Separate providers	9
Power connection types.....	9
Cable management	10
Network cabling	11
Redundant networking.....	11
Copper cabling.....	11
Fiber optic cabling	11
Fiber optic cable connectors	12
Gigabit networks	12
Small form-factor pluggable.....	13
Server chassis types.....	13
Tower chassis	13
Rack mount chassis	13
Blade chassis.....	14

Server components.....	14
<i>Hardware compatibility list</i>	14
Central Processing Unit.....	15
Instruction sets	15
CPU vs. cores.....	15
Graphics Processing Unit	16
Memory	16
Server interfaces	17
Hardware interfaces	17
Software interfaces	17
User interfaces.....	18
Conclusion.....	18
Points to remember	19
2. Data Storage	21
Introduction.....	21
Structure.....	21
Objective	22
Hard disk drives.....	22
<i>Hard disk drive specifications</i>	22
Hard drive interfaces	23
Interface types	23
Serial ATA.....	24
Serial Attached SCSI (SAS)	24
Peripheral Component Interconnect.....	25
Universal Serial Bus	25
Secure Digital Card.....	26
RAID levels and types	27
Striping and mirroring	27
RAID levels	27
Just a bunch of disks	29
Hardware RAID versus software RAID.....	29
Capacity planning	30
Disk drive media	30
Solid-State devices.....	31
Wear factors	31

<i>Use factors</i>	32
Shared storage.....	32
<i>Network attached storage</i>	32
<i>Storage area network</i>	33
Conclusion.....	34
Points to remember	34
3. Server Hardware Maintenance.....	37
Introduction.....	37
Structure.....	37
Objective	38
Out-of-band management.....	38
Local hardware administration.....	39
<i>Keyboard-Video-Mouse (KVM)</i>	39
<i>Crash cart</i>	40
<i>Virtual administration console</i>	40
<i>Serial connectivity</i>	40
<i>Console connections</i>	41
Drive maintenance	41
Hot-swappable hardware	43
<i>Hot-swappable devices</i>	43
<i>Cold-swappable devices</i>	44
Firmware upgrades.....	44
BIOS/UEFI maintenance.....	44
<i>Flashing BIOS</i>	45
<i>Flashing UEFI</i>	45
Conclusion.....	45
Points to remember	46
Part - 2: Server Administration	47
4. Server Operating Systems	49
Introduction.....	49
Structure.....	49
Objective	50
Minimum hardware requirements	50

Windows Server 2022	50
Windows 10/11.....	50
Linux distros	51
Hardware compatibility list	51
Operating system installations.....	52
Installation types.....	52
OS Core.....	53
Bare Metal.....	53
Virtualized.....	53
Remote Server Administration	54
Slipstreaming	56
Unattended installations.....	56
Scripted installations	56
Installation media types.....	56
Imaging	57
Cloning.....	57
Software deployment templates.....	58
Partition and volume types	58
Master boot record	59
GUID partition	59
Dynamic disk	60
Logical volume management.....	60
File system types	61
File systems	61
ext4.....	61
NTFS.....	63
Virtual Machine File System	63
Resilient File System.....	63
Storage Spaces.....	64
Z File system	64
Conclusion.....	64
Points to remember	65
5. Network Infrastructure Services	67
Introduction.....	67
Structure.....	67

Objective	68
IP configuration	68
<i>The Windows ipconfig command</i>	69
DNS.....	70
<i>Hosts</i>	71
DHCP	72
APIPA	72
<i>The Linux ifconfig command</i>	72
<i>The Linux ip command</i>	73
Addresses.....	74
Routes.....	75
Links	76
Neighbors	76
Virtual local area networks	77
Default gateways	78
Addressing protocols.....	78
MAC addressing	78
Internet Protocol addressing	79
IPv4.....	79
IPv6.....	82
Firewalls.....	83
<i>Firewall types</i>	83
<i>Firewall methods</i>	83
<i>Firewall ports</i>	84
Conclusion.....	85
Points to remember	85
6. Configure Network Servers.....	87
Introduction.....	87
Structure.....	87
Objective	88
Server roles and requirements.....	88
<i>Print server</i>	88
<i>Database server</i>	89
<i>File server</i>	89

Web server	89
Application server	90
Messaging servers	91
Server baselining	91
Directory connectivity	92
Storage management	93
Processes	93
Formatting	94
Partitioning	95
Paging	95
Windows	95
Linux and macOS	96
Scratch space	96
Disk quotas	96
Compression	97
Lossy compression	97
Lossless compression	98
Windows file compression	98
Linux file compression	99
Deduplication	99
Server monitoring	100
Log files	101
Windows logs	101
Linux logs	103
Monitoring	104
Monitoring types	104
Monitoring tools	104
Performance monitoring	104
Data migration and transfer	106
Administrative interfaces	107
KVM interfaces	107
Network-based interfaces	108
Conclusion	108
Points to remember	109

7. High Availability.....	111
Introduction.....	111
Structure.....	111
Objective	112
High availability	112
Fault tolerance.....	113
<i>Swaps</i>	114
Clustering	114
<i>Server clusters</i>	115
Load balancing.....	115
<i>Path selection policy</i>	116
<i>NIC teaming and redundancy</i>	117
<i>NIC teaming modes</i>	117
Conclusion.....	118
Points to remember	118
8. Virtualization	121
Introduction.....	121
Structure.....	121
Objective	122
Virtualization	122
Host vs. guest.....	122
<i>Virtual networking</i>	124
<i>Network address translation</i>	125
<i>Direct access</i>	125
<i>Virtual NIC</i>	125
Resource allocation and provisioning	126
<i>CPU allocation</i>	126
<i>Memory allocation</i>	127
<i>Disk allocation</i>	127
<i>Overprovisioning</i>	128
VM testing	128
<i>VM management interfaces</i>	129
Cloud models.....	130
<i>Private cloud</i>	130

<i>Public cloud</i>	130
<i>Hybrid cloud</i>	131
<i>Community cloud</i>	131
Conclusion.....	132
Points to remember	132
9. Scripting	133
Introduction.....	133
Structure.....	133
Objective	134
Scripting in server administration	134
<i>Script uses</i>	134
Script types.....	135
Basic scripting constructs	136
Scripting terminology.....	136
Basic data types	137
Server administration scripting.....	138
<i>Windows scripts</i>	138
<i>Windows startup scripts</i>	138
<i>Windows shutdown scripts</i>	142
<i>Start/stop services</i>	142
<i>User logins</i>	143
<i>Account creation</i>	143
Windows environmental variables.....	144
Script comments	145
Linux scripts.....	146
<i>Linux startup scripts</i>	146
<i>Crontab</i>	146
<i>Permissions</i>	147
<i>Linux shutdown scripts</i>	147
<i>User logins/logouts</i>	147
<i>Account creation</i>	148
Linux environmental variables	149
<i>Linux script comments</i>	149
Conclusion.....	150
Points to remember	150

10. Asset Management.....	151
Introduction.....	151
Structure.....	151
Objective	152
Asset management	152
<i>Asset management process.....</i>	<i>152</i>
<i>Asset lifecycle</i>	<i>152</i>
<i>Asset labeling</i>	<i>153</i>
<i>Asset classification</i>	<i>154</i>
Documentation management	154
<i>Internal documentation.....</i>	<i>155</i>
<i>Documentation updates</i>	<i>155</i>
<i>Documentation content.....</i>	<i>155</i>
<i>Document availability.....</i>	<i>156</i>
Change management	157
Policies and procedures	157
Conclusion	159
Points to remember	159
11. Licensing.....	161
Introduction.....	161
Structure.....	161
Objective	161
Software licensing	162
<i>Licensing agreements</i>	<i>162</i>
<i>Licensing models</i>	<i>162</i>
<i>Subscriptions.....</i>	<i>164</i>
<i>Software license and maintenance agreements</i>	<i>164</i>
<i>Volume licensing.....</i>	<i>165</i>
<i>License validation.....</i>	<i>165</i>
Version compatibility	166
Conclusion.....	168
Points to remember	168

Part - 3: Security and Disaster Recovery	171
12. Data Security	173
Introduction.....	173
Structure.....	173
Objective	174
Encryption	174
<i>Data encryption</i>	174
<i>Data-at-rest</i>	175
<i>Data-in-transit</i>	175
<i>Data-in-Use</i>	176
Data retention policies	176
Data storage.....	177
Data protection and data security	177
<i>Data protection</i>	177
<i>Data security</i>	178
<i>Data security compliance</i>	179
<i>Storage security</i>	181
<i>On-site storage</i>	181
<i>Off-site storage</i>	182
<i>System passwords</i>	183
<i>BIOS/UEFI passwords</i>	183
<i>Bootloader password</i>	183
Business impacts.....	184
<i>Data value prioritization</i>	185
<i>Data life-cycle management</i>	185
<i>Cybersecurity costs versus risks</i>	186
Conclusion.....	187
Points to remember	187
13. Physical Security	189
Introduction.....	189
Structure.....	189
Objective	190
Access controls.....	190
<i>Physical access</i>	190

<i>External perimeter security</i>	190
<i>Bollards</i>	191
Architectural security reinforcements	191
<i>Signal blocking</i>	191
<i>Reflective glass</i>	193
<i>Data center camouflage</i>	193
<i>Security fencing</i>	193
<i>Security cameras</i>	194
<i>Locks</i>	195
<i>Key cards</i>	195
Authentication factors	196
<i>Mantraps and tailgating</i>	197
<i>Multifactor Authentication</i>	197
Environmental controls	198
<i>Environmental monitoring</i>	198
<i>Environmental threats</i>	199
Conclusion	199
Points to remember	200
14. Access Management	203
Introduction	203
Structure	203
Objective	204
User accounts	204
<i>Default local accounts</i>	204
<i>Local user account types</i>	205
<i>User groups</i>	205
<i>Linux user accounts</i>	206
<i>Linux user groups</i>	207
Access controls	207
Permissions	207
<i>Delegation</i>	208
<i>Password policies</i>	208
<i>Separation of duties</i>	209
Auditing	209

Access control audits.....	210
User activity audits.....	211
User account management.....	211
User account logins.....	212
Group memberships	212
Deletions	213
Auditing Linux systems.....	214
Single sign-on.....	216
Conclusion.....	216
Points to remember	217
15. Risk and Mitigation.....	219
Introduction.....	219
Structure.....	219
Objective	220
Security risks	220
Vulnerabilities	221
Threat actors.....	221
Threat actor motivations	222
Common attacks	223
Data center risks.....	224
Data theft.....	224
Data loss prevention.....	225
Data duplication.....	226
In-line and post-process deduplication.....	227
Source and target deduplication.....	227
Hardware-based and software-based deduplication	227
Data publication.....	227
Unwanted access methods.....	228
Backdoor	229
Identifying and disclosing data breaches.....	229
Mitigation strategies	230
Proactive strategies.....	231
Attack surfaces	232
Security information and event management.....	232

Log management	232
Two-person integrity.....	233
Split encryption keys and tokens	233
Separation of roles	233
Regulatory constraints.....	234
Payment Card Industry Data Security Standard.....	235
General Data Protection Regulation.....	235
The Red Flags rule.....	235
Data retention	236
Conclusion.....	236
Points to remember	237
16. Server Hardening and Decommissioning.....	239
Introduction.....	239
Structure.....	239
Objective	240
Hardening	240
Server OS hardening.....	240
Firewall and Router hardening.....	241
Firewall hardening.....	241
Router hardening.....	241
Workstation hardening.....	242
Application hardening.....	242
Host security	242
Hardware hardening	243
Patch management	244
Change management	245
Server decommissioning.....	245
Media destruction	246
Media retention requirements	248
Backup media.....	248
Backup media retention	248
Cable remediation	249
Electrical wiring.....	249
Computer cabling.....	249

Electronics recycling	250
<i>Internal vs. external recycling</i>	250
<i>Repurposing</i>	251
Conclusion.....	251
Points to remember	251
17. Backup and Restore	253
Introduction.....	253
Structure.....	253
Objective	253
Backup and recovery	254
<i>Backup methods</i>	254
<i>Backup types</i>	254
<i>Backup strategies</i>	256
<i>The 3-2-1 backup strategy</i>	256
<i>Grandfather-father-son backups</i>	256
<i>Archive vs. Backup</i>	257
<i>Open files</i>	257
<i>File-level vs. system-state backup</i>	258
Restore methods	258
<i>Overwrite</i>	259
<i>Side by side</i>	259
<i>Task Scheduler</i>	260
<i>Disk Cleanup</i>	261
Backup validation.....	262
<i>Media integrity</i>	262
<i>Backup storage devices</i>	263
<i>Regular testing intervals</i>	263
<i>Media inventory before restoration</i>	263
Conclusion.....	263
Points to remember	264
18. Disaster Recovery	265
Introduction.....	265
Structure.....	265
Objective	266

Disaster recovery planning.....	266
Recovery sites.....	267
Replication.....	268
Testing.....	270
Failovers and failbacks.....	271
<i>Failover</i>	271
<i>Failback</i>	272
<i>Failover simulation</i>	272
Testing: Production vs. non-production.....	273
Conclusion.....	273
Points to remember.....	274

Part - 4: Troubleshooting..... 275

19. Troubleshooting Methods.....	277
Introduction.....	277
Structure.....	277
Objective.....	278
Troubleshooting step.....	278
<i>Soft skills</i>	278
Identifying the problem and determining the scope.....	279
<i>Hardware or software?</i>	279
<i>Hardware problems</i>	280
<i>Software problems</i>	280
Establishing a theory of probable cause.....	281
Testing the theory to determine the cause.....	282
Establishing a plan of action to resolve the problem.....	282
<i>Repair work plan</i>	282
<i>Identifying potential effects</i>	283
<i>Implementing the solution or escalate</i>	283
Verification and prevention.....	284
<i>Verifying full system functionality</i>	284
<i>Implementing preventive measures</i>	284
Performing Root Cause analysis.....	285
Document findings, actions, and outcomes throughout the process.....	285

Conclusion.....	286
Points to remember	286
20. Hardware Issues	289
Introduction.....	289
Structure.....	289
Objective	290
Common hardware problems.....	290
<i>Predictive failures</i>	290
<i>Memory issues</i>	291
<i>Memory troubleshooting</i>	291
<i>Common memory errors and failures</i>	292
<i>Blue Screen of Death</i>	292
<i>Purple screen</i>	293
<i>Memory utilization</i>	293
<i>Using Task Manager to check memory</i>	294
<i>Command to check memory utilization</i>	295
<i>POST errors</i>	296
<i>Random lockups</i>	297
<i>Kernel panic</i>	299
<i>CMOS battery failure</i>	299
<i>Fault and device indication</i>	300
<i>Problem sounds and smells</i>	301
<i>Misallocated virtual resources</i>	303
<i>Common problem causes</i>	303
<i>Power supply unit</i>	303
<i>Malfunctioning fans</i>	304
<i>Cooling fans</i>	304
<i>Common fan issues</i>	306
<i>Overheating issues</i>	306
<i>Heat sink issues</i>	306
<i>Improperly seated expansion cards</i>	307
<i>Windows event logs</i>	309
<i>Hardware diagnostics</i>	312
<i>Electrostatic discharge equipment</i>	312

Conclusion.....	314
Points to remember	314
21. Storage Issues.....	317
Introduction.....	317
Structure.....	317
Objective	317
Common storage device problems	318
<i>Common disk drive problems</i>	<i>319</i>
Causes of common problems.....	322
<i>Virtual memory problems.....</i>	<i>322</i>
<i>Media failures.....</i>	<i>323</i>
<i>Hard disk media</i>	<i>323</i>
<i>SSD media.....</i>	<i>323</i>
<i>Magnetic tape media.....</i>	<i>324</i>
Causes of common storage problems.....	324
<i>Disk space utilization</i>	<i>324</i>
<i>Drive and connector failures.....</i>	<i>325</i>
<i>Disk drive problems.....</i>	<i>325</i>
<i>Cable and connector problems.....</i>	<i>326</i>
<i>Storage system issues</i>	<i>327</i>
<i>Software-caused failures.....</i>	<i>327</i>
<i>Hardware-based issues</i>	<i>328</i>
<i>Storage array issues</i>	<i>329</i>
Administrative tools.....	329
Disk management.....	330
Map, mount, and net use	330
Disk arrays.....	331
Storage monitoring tools.....	333
Visual and auditory inspections.....	334
Conclusion.....	335
Points to remember	335
22. Operating System and Software Issues.....	337
Introduction.....	337
Structure.....	337

Objective	337
Common OS and software problems	338
<i>Hardware-related software problems</i>	338
<i>Common OS problems</i>	339
Causes of common problems	342
<i>End of life/end of support</i>	342
<i>User account controls</i>	342
<i>Access control</i>	343
Windows	343
Linux and macOS	344
Corrupted files	345
Windows file recovery	345
Linux file recovery	346
Log files	346
Incompatible drivers	347
Improperly applied patches	349
Server not joined to a domain	349
Clock skew	350
Buffer overrun	350
Insecure dependencies	350
Version management	351
Architecture	351
Missing updates	352
Downstream failures caused by updates	353
Improper CPU affinity and priority	354
CPU affinity	354
Priority	355
Conclusion	356
Points to remember	356
23. Software Tools and Techniques	359
Introduction	359
Structure	359
Objective	359
Tools and techniques	360

<i>Adding or removing ports</i>	360
<i>Boot options</i>	363
<i>Clocks</i>	364
<i>Configuration management</i>	365
<i>Configuration assessment</i>	365
<i>Drift analysis</i>	365
<i>Chef, Puppet, and Ansible</i>	366
<i>Downgrades</i>	367
<i>Group Policy Object</i>	367
<i>Network time protocol</i>	368
<i>Package management</i>	368
<i>Patching</i>	368
<i>Privilege escalation</i>	369
<i>Reloading an OS</i>	369
<i>Run as command</i>	369
<i>Safe mode</i>	371
<i>Scheduled reboots</i>	372
<i>Windows OS</i>	372
<i>Linux OS</i>	373
<i>Software firewalls</i>	374
<i>Status identification</i>	374
<i>Stopping: kill a stuck service</i>	375
<i>Windows</i>	375
<i>Linux</i>	376
<i>System Center Configuration Manager</i>	376
<i>Zones</i>	376
<i>DNS Zones</i>	377
<i>Security zones</i>	377
<i>Conclusion</i>	379
<i>Points to remember</i>	379
24. Network Connectivity Issues	381
<i>Introduction</i>	381
<i>Structure</i>	381
<i>Objective</i>	382
<i>Common network problems</i>	382

<i>Internet connectivity</i>	382
<i>Network resource unavailable</i>	383
<i>Configuration problems</i>	384
<i>DHCP server</i>	384
<i>APIPA</i>	385
<i>Destination host unreachable</i>	385
<i>Unknown host</i>	385
<i>Unable to reach remote subnets</i>	386
<i>Failure of service provider</i>	386
<i>Cannot reach server</i>	387
<i>DNS record types</i>	387
<i>Cannot reach server using hostname</i>	389
<i>Cannot reach server using FQDN</i>	389
<i>Causes of common problems</i>	389
<i>Improper IP configuration</i>	390
<i>IPv4 vs. IPv6 misconfigurations</i>	390
<i>Network port security</i>	391
<i>Component failures</i>	391
<i>Incorrect OS route tables</i>	392
<i>Routing tables</i>	392
<i>Routes</i>	394
<i>Routing table errors</i>	394
<i>Troubleshooting tools</i>	394
<i>Device misconfiguration</i>	394
<i>Misconfigured NIC</i>	395
<i>System resources</i>	396
<i>VLAN configuration errors</i>	397
<i>Default gateway not available</i>	398
<i>Firewall failure</i>	398
<i>Power supply issues</i>	399
<i>Conclusion</i>	400
<i>Points to remember</i>	400
25. Network Tools and Techniques	403
<i>Introduction</i>	403
<i>Structure</i>	403

Objective	404
Troubleshooting tools	404
<i>Check link lights</i>	404
<i>Confirm power supply</i>	404
<i>Verify cable integrity</i>	405
<i>Cable selection</i>	405
Troubleshooting commands	407
<i>ipconfig/ifconfig</i>	407
Windows	407
Linux/macOS	408
<i>ip</i>	408
<i>Ping</i>	410
<i>Tracert/traceroute</i>	410
<i>nslookup</i>	411
<i>nbtstat</i>	411
<i>nbtscan</i>	412
<i>nmblookup</i>	413
<i>netstat</i>	413
<i>dig</i>	414
<i>Telnet</i>	414
<i>Netcat</i>	414
<i>route</i>	415
<i>Routing table</i>	416
<i>Add, change, or remove routes</i>	418
Conclusion	418
Points to remember	419
26. Troubleshooting Security Issues	421
Introduction	421
Structure	421
Objective	421
Common data security concerns	422
<i>Common security issue causes</i>	425
<i>Active services</i>	425
<i>Inactive accounts</i>	426

<i>Anti-malware configurations</i>	426
<i>Misconfigured permissions</i>	426
<i>Open ports</i>	427
<i>Rogue processes/services</i>	427
<i>Zombie/orphan</i>	428
<i>Intrusion detection configurations</i>	428
<i>Improperly configured local/group policies</i>	429
<i>Misconfigured firewall rules</i>	430
Commonly used security tools.....	431
<i>Anti-malware and antivirus</i>	433
<i>Monitoring vs. detection</i>	434
<i>Monitoring</i>	434
<i>Detecting</i>	435
<i>User access controls</i>	437
<i>Windows</i>	437
<i>Linux/macOS</i>	438
<i>User account control</i>	438
<i>Security-enhanced Linux</i>	438
Conclusion.....	439
Points to remember	439
 Appendix A: CompTIA Server+ Certification Exam: Practice Test 1	441
Appendix B: CompTIA Server+ Certification Exam: Practice Test 2.....	459
Appendix C: CompTIA Server+® Acronyms	477
Appendix D: Key Terms/ Concepts.....	485
Appendix E: Answers to Practice Test 1	515
Appendix F: Answers to Practice Test 2	519
 Index	523-535

Part - 1

Server Hardware Installation and Management

Regardless of its purpose or role in a network, a server has two primary components: hardware and software. In this part, you review the system and data storage hardware, their installation, function, and maintenance.

Part 1 includes the following chapters:

- Chapter 1: Physical Hardware
- Chapter 2: Storage Devices
- Chapter 3: Server Hardware Maintenance

CHAPTER 1

Physical Hardware

Introduction

When we think about a network server, we lump the hardware and software into one system. For the most part, this is not entirely wrong, but technically, a server is a software and its support services. We commonly refer to the physical hardware as a server, even though it could have multiple server software running on it. In this chapter and the whole book, the term server is used interchangeably to indicate both. Keep in mind that there is some difference between server hardware and server software. So, it is okay to see a server as the combination of the hardware and the software in the context of the service it provides to a network. Regardless, without its hardware or its software, there would be no server.

This chapter focuses on the server's internal and external components, racking, cabling, and support hardware. The hardware discussed in this chapter (and most of this book), is generally associated with larger networks and data centers. However, all servers, even the **small offices or home offices (SOHO)**, require the same support systems, in one form or another. With that understanding, let us look at the various types of hardware and support systems that provide for the operations of a server.

Structure

The chapter covers the following topics:

- Racking systems
- Power cabling
- Network cabling
- Server chassis types
- Server components

Objective

By the end of this chapter, you will be able to identify and describe the sub-objectives of the following Server+ examination objective: *Given a scenario, install physical hardware.*

Racking systems

The hardware on which server software runs can be a standalone computer or a computer system specifically designed for that purpose. The computers/servers in large networks are commonly contained in specially designed computer rooms, data centers, or server farms. In these environments, the server hardware is typically mounted on open racks or in cabinets. *Figure 1.1* shows examples of an open rack and a rackmount cabinet like those commonly found in data centers:



Figure 1.1: Server hardware is commonly mounted on an open rack (left) or a server cabinet (right) in large data centers ¹

1. Images courtesy of Datarack Co.

Rack dimensions

The dimensions of a mountable rack device have a standard width and height sizing. The majority of rackmount devices have a width of 19-inches, but their heights can vary with the type and purpose of each device. Racking systems, like those shown in *Figure 1.1*, have either two or four vertical rails. Server hardware and other devices are attached to the rails using a rail kit. A rail kit is typically specific to the device with horizontally mounted rails on which the device sits, and fasteners to secure the device to the vertical rails. A two-rail rack has no depth limitations, but a four-rail rack is typically either 24 or 48-inches in-depth and is designed to enclose devices.

Rackmount systems are designed to accommodate varying device heights. The height of a device is measured using the rack unit or “U.” One U, or “1U,” is standardized at 1.75 inches. *Figure 1.2* illustrates the size of 1U. Most racks or cabinet systems are 42U in height. Rack-mountable server hardware is 2U or 3.5U tall. Theoretically, twenty-one 2U devices could be mounted in a 42U rack:

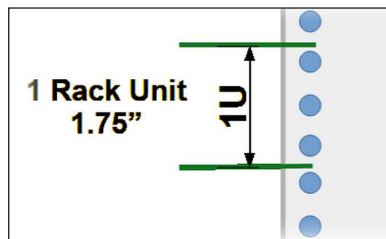


Figure 1.2: One rack unit (1U) is 1.75 inches in height

Rack layout

Racking systems are designed to hold all standard rack-mountable devices, including server hardware, **uninterruptible power supplies (UPS)**, **power distribution units (PDUs)**, cable management devices, **keyboard-video-mouse (KVM)** switches, patch panels, and more. However, the placement of certain devices can affect the effectiveness of the cooling system and its airflow.

Before inserting devices into a rack, you should plan where each device should be in relationship to the other devices. If there are multiple racks, consider the power and cooling systems of the facility. Heavier devices, such as a UPS, should be placed at the bottom of the rack, and the lightest devices should tend toward the top. Devices common to a rack installation, such as patch panels, routers, switches, firewalls, etc., are typically placed in the upper part of the rack. This is for the ease of installation, access, and cable management.