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

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 informaiton 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 successul 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

Rack dimensions 5

Rack layout 5

Cooling management 6

Safety 6

Power Distribution Unit 7

Keyboard-Video-Mouse 7

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
Hardware compatibility list 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
Hard disk drive specifications 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

Use factors 32
Shared storage 32
Network attached storage 32
Storage area network 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
Keyboard-Video-Mouse (KVM) 39
Crash cart 40
Virtual administration console 40
Serial connectivity 40
Console connections 41
Drive maintenance 41
Hot-swappable hardware 43
Hot-swappable devices 43
Cold-swappable devices 44
Firmware upgrades 44
BIOS/UEFI maintenance 44
Flashing BIOS 45
Flashing UEFI 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
The Windows ipconfig command 69
DNS 70
Hosts 71
DHCP 72
APIPA 72
The Linux **ifconfig** *command* 72
The Linux ip *command* 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
Firewall types 83
Firewall methods 83
Firewall ports 84
Conclusion 85
Points to remember 85

6. Configure Network Servers 87
Introduction 87
Structure 87
Objective 88
Server roles and requirements 88
Print server 88
Database server 89
File server 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

Swaps......114

Clustering 114

Server clusters 115

Load balancing......115

Path selection policy......116

NIC teaming and redundancy......117

NIC teaming modes......117

Conclusion......118

Points to remember 118

8. Virtualization 121

Introduction......121

Structure......121

Objective 122

Virtualization 122

Host vs. guest......122

Virtual networking......124

Network address translation 125

Direct access......125

Virtual NIC......125

Resource allocation and provisioning 126

CPU allocation 126

Memory allocation......127

Disk allocation......127

Overprovisioning 128

VM testing 128

VM management interfaces 129

Cloud models......130

Private cloud 130

Public cloud ... *130*

Hybrid cloud ... *131*

Community cloud ... *131*

Conclusion ... 132

Points to remember ... 132

9. Scripting ... 133

Introduction ... 133

Structure ... 133

Objective ... 134

Scripting in server administration ... 134

Script uses ... *134*

Script types ... 135

Basic scripting constructs ... 136

Scripting terminology ... 136

Basic data types ... 137

Server administration scripting ... 138

Windows scripts ... *138*

Windows startup scripts ... *138*

Windows shutdown scripts ... *142*

Start/stop services ... *142*

User logins ... *143*

Account creation ... *143*

Windows environmental variables ... 144

Script comments ... 145

Linux scripts ... 146

Linux startup scripts ... *146*

Crontab ... *146*

Permissions ... *147*

Linux shutdown scripts ... *147*

User logins/logouts ... *147*

Account creation ... *148*

Linux environmental variables ... 149

Linux script comments ... *149*

Conclusion ... 150

Points to remember ... 150

10. Asset Management.. 151

Introduction.. 151

Structure.. 151

Objective 152

Asset management 152

Asset management process.. 152

Asset lifecycle 152

Asset labeling 153

Asset classification 154

Documentation management 154

Internal documentation.. 155

Documentation updates 155

Documentation content.. 155

Document availability 156

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

Licensing agreements 162

Licensing models 162

Subscriptions.. 164

Software license and maintenance agreements 164

Volume licensing.. 165

License validation.. 165

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

Data encryption 174

Data-at-rest 175

Data-in-transit 175

Data-in-Use 176

Data retention policies 176

Data storage 177

Data protection and data security 177

Data protection 177

Data security 178

Data security compliance 179

Storage security 181

On-site storage 181

Off-site storage 182

System passwords 183

BIOS/UEFI passwords 183

Bootloader password 183

Business impacts 184

Data value prioritization 185

Data life-cycle management 185

Cybersecurity costs versus risks 186

Conclusion 187

Points to remember 187

13. Physical Security 189

Introduction 189

Structure 189

Objective 190

Access controls 190

Physical access 190

External perimeter security 190

Bollards 191

Architectural security reinforcements 191

Signal blocking 191

Reflective glass 193

Data center camouflage 193

Security fencing 193

Security cameras 194

Locks 195

Key cards 195

Authentication factors 196

Mantraps and tailgating 197

Multifactor Authentication 197

Environmental controls 198

Environmental monitoring 198

Environmental threats 199

Conclusion 199

Points to remember 200

14. Access Management 203

Introduction 203

Structure 203

Objective 204

User accounts 204

Default local accounts 204

Local user account types 205

User groups 205

Linux user accounts 206

Linux user groups 207

Access controls 207

Permissions 207

Delegation 208

Password policies 208

Separation of duties 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
Internal vs. external recycling *250*
Repurposing *251*
Conclusion........ 251
Points to remember 251

17. Backup and Restore 253
Introduction........ 253
Structure........ 253
Objective 253
Backup and recovery 254
Backup methods *254*
Backup types *254*
Backup strategies *256*
The 3-2-1 backup strategy *256*
Grandfather-father-son backups *256*
Archive vs. Backup *257*
Open files *257*
File-level vs. system-state backup *258*
Restore methods 258
Overwrite *259*
Side by side *259*
Task Scheduler *260*
Disk Cleanup *261*
Backup validation........ 262
Media integrity *262*
Backup storage devices *263*
Regular testing intervals *263*
Media inventory before restoration *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
Failover *271*
Failback *272*
Failover simulation *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
Soft skills *278*
Identifying the problem and determining the scope 279
Hardware or software? *279*
Hardware problems *280*
Software problems *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
Repair work plan *282*
Identifying potential effects *283*
Implementing the solution or escalate *283*
Verification and prevention 284
Verifying full system functionality *284*
Implementing preventive measures *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
Predictive failures 290
Memory issues 291
Memory troubleshooting 291
Common memory errors and failures 292
Blue Screen of Death 292
Purple screen 293
Memory utilization 293
Using Task Manager to check memory 294
Command to check memory utilization 295
POST errors 296
Random lockups 297
Kernel panic 299
CMOS battery failure 299
Fault and device indication 300
Problem sounds and smells 301
Misallocated virtual resources 303
Common problem causes 303
Power supply unit 303
Malfunctioning fans 304
Cooling fans 304
Common fan issues 306
Overheating issues 306
Heat sink issues 306
Improperly seated expansion cards 307
Windows event logs 309
Hardware diagnostics 312
Electrostatic discharge equipment 312

Conclusion 314

Points to remember 314

21. Storage Issues 317

Introduction 317

Structure 317

Objective 317

Common storage device problems 318

Common disk drive problems 319

Causes of common problems 322

Virtual memory problems 322

Media failures 323

Hard disk media 323

SSD media 323

Magnetic tape media 324

Causes of common storage problems 324

Disk space utilization 324

Drive and connector failures 325

Disk drive problems 325

Cable and connector problems 326

Storage system issues 327

Software-caused failures 327

Hardware-based issues 328

Storage array issues 329

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
Hardware-related software problems *338*
Common OS problems *339*
Causes of common problems 342
End of life/end of support *342*
User account controls *342*
Access control *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

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

24. Network Connectivity Issues 381
Introduction 381
Structure 381
Objective 382
Common network problems 382

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

25. Network Tools and Techniques 403
Introduction 403
Structure 403

Objective 404
Troubleshooting tools 404
Check link lights *404*
Confirm power supply *404*
Verify cable integrity *405*
Cable selection *405*
Troubleshooting commands 407
ipconfig/ifconfig *407*
Windows *407*
Linux/macOS *408*
ip *408*
Ping *410*
Tracert/traceroute *410*
nslookup *411*
nbtstat *411*
nbtscan *412*
nmblookup *413*
netstat *413*
dig *414*
Telnet *414*
Netcat *414*
route *415*
Routing table *416*
Add, change, or remove routes *418*
Conclusion 418
Points to remember 419

26. Troubleshooting Security Issues 421
Introduction 421
Structure 421
Objective 421
Common data security concerns 422
Common security issue causes *425*
Active services *425*
Inactive accounts *426*

Anti-malware configurations ... *426*
Misconfigured permissions ... *426*
Open ports ... *427*
Rogue processes/services ... *427*
Zombie/orphan ... *428*
Intrusion detection configurations ... *428*
Improperly configured local/group policies ... *429*
Misconfigured firewall rules ... *430*
Commonly used security tools ... 431
Anti-malware and antivirus ... *433*
Monitoring vs. detection ... *434*
Monitoring ... *434*
Detecting ... *435*
User access controls ... *437*
Windows ... *437*
Linux/macOS ... *438*
User account control ... *438*
Security-enhanced Linux ... *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:

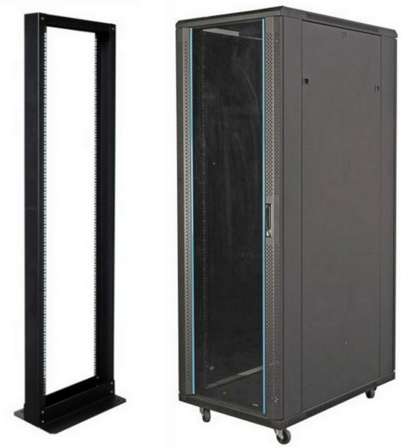

Figure 1.1*: Server hardware is commonly mounted on an open rack (left) or a server cabinet (right) in large data centers* [1]

[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 3.5-inches tall. Theoretically, twenty-one 2U devices could be mounted in a 42U rack:

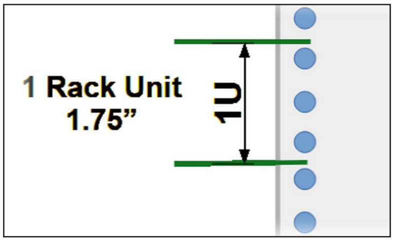

***Figure 1.2**: One rack unit (1U) is 1.75 inches in height*

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.