

Inhaltsverzeichnis

1	Einführung	17
1.1	Das Ziel dieses Buches	17
1.2	Die CompTIA Server+-Zertifizierung	18
1.3	Voraussetzungen für CompTIA Server+	19
1.4	Die Autoren	19
1.5	Sind Sie bereit für CompTIA Server+?	20
2	Was ist ein Server?	27
2.1	Server als Definitionssache	27
2.2	Von Hosts und Servern	30
2.3	Warum ein PC kein Server ist	32
2.4	Bauformen von Servern	34
2.5	Alles eine Frage der Höheneinheit	37
2.6	KVMs	40
2.7	Fragen zu diesem Kapitel	41
3	Serverhardware	43
3.1	Die Architektur von Servern	43
3.1.1	Alt, aber noch vorhanden: PCI	44
3.1.2	PCI-X	46
3.1.3	PCI-Express	47
3.1.4	Die Weiterentwicklungen bei Intel	50
3.1.5	Die Bussysteme im Vergleich	52
3.1.6	Chipsets im Vergleich	52
3.2	Prozessoren für Server	53
3.2.1	Technische Funktion der CPU	57
3.2.2	Hardwarevirtualisierung via Prozessor	58
3.2.3	Mehrkernprozessoren	58
3.2.4	Cache-Speicher (Pufferspeicher)	59
3.3	Der Arbeitsspeicher	60
3.3.1	Unterschiedliche Funktionsweisen	60
3.3.2	Aufbau von RAM-Bausteinen	61
3.3.3	Fehlerbehandlung	62
3.3.4	Aktuelle RAM-Typen	63

3.3.5	Single Channel, Dual Channel, Quad Channel	67
3.3.6	Bauformen	68
3.4	Kühlung von Servern.	69
3.4.1	Wärmeleitpaste	70
3.4.2	Lüfter	70
3.4.3	Kühlkörper	71
3.4.4	Wasserkühlung	71
3.5	Hot-Plug-Architekturen.	72
3.6	BIOS in ROM?	74
3.6.1	Der POST im Detail	75
3.6.2	EFI und UEFI	77
3.6.3	Fehlermeldungen	78
3.7	Fragen zu diesem Kapitel	79
4	Storage-Lösungen	81
4.1	Die Hardware drunter	81
4.2	Solid State Drives (SSD)	84
4.2.1	MLC oder SLC.	85
4.2.2	Hybrid-Festplatten (Hybrid Hard Drives).	86
4.2.3	Anschlussmöglichkeiten	86
4.2.4	Einsatz in Servern.	86
4.3	SCSI	86
4.3.1	Architektur	87
4.3.2	SCSI-Kabel und -Stecker	90
4.3.3	SCSI-Standards.	91
4.4	Es werde seriell – SATA	92
4.4.1	Unterschied zu PATA.	93
4.4.2	Stecker und Kabel	93
4.5	SAS	96
4.5.1	Übertragungstechnik	98
4.5.2	Single- und Dual-Port.	98
4.5.3	SAS-Stecker und -Kabel	98
4.6	Fibre Channel.	99
4.6.1	Architekturen	100
4.6.2	Fibre Channel over Ethernet	103
4.7	iSCSI.	103
4.8	DAS und NAS	104
4.9	Storage Area Network	106
4.10	Fragen zu diesem Kapitel	108

5	Stabilität durch Fehlertoleranz	111
5.1	RAID	111
5.1.1	RAID-Level	112
5.1.2	Duplexing	118
5.1.3	Übersicht RAID	118
5.2	Energieversorgung	119
5.2.1	Grundlegende Betrachtungen	120
5.2.2	USV	121
5.2.3	Notstromgruppen	123
5.2.4	Einsatzszenarien	124
5.2.5	Rotationsenergiestromversorgungen	125
5.3	Clustering	125
5.3.1	Network Loadbalancing	126
5.3.2	Multiprocessing	126
5.3.3	Cluster	127
5.4	Hardwareredundanz	128
5.4.1	Steckkarten	128
5.4.2	Netzteile (Power Supply)	128
5.4.3	Kühlsystem/Lüfter	129
5.4.4	Arbeitsspeicher	130
5.5	Fragen zu diesem Kapitel	130
6	Server installieren und aktualisieren	133
6.1	Sicherheitsmaßnahmen	133
6.1.1	Statische Entladung (ESD)	133
6.1.2	MSDS	135
6.1.3	Heben und Tragen	135
6.2	Installation eines Servers	136
6.2.1	Der Installationsplan	136
6.2.2	Dokumentation	137
6.3	Server umbauen	139
6.4	Was bei einem Umbau zu beachten ist	140
6.4.1	Ersatz des Motherboards	140
6.4.2	Prozessor	141
6.4.3	BIOS	143
6.4.4	Speicheraufrüstung	145
6.4.5	Festplatten	146
6.4.6	SATA-/SAS-Controller	146

6.4.7	Erweiterungskarten	147
6.5	Fragen zu diesem Kapitel	148
7	Hardware im Netzwerk	151
7.1	Die wichtigsten Übertragungsmedien	151
7.1.1	Twisted-Pair-Kabel	153
7.1.2	Unshielded Twisted Pair	155
7.1.3	Shielded Twisted Pair	160
7.1.4	Koaxialkabel.	162
7.1.5	Lichtwellenleiter	163
7.2	Netzwerkkarten	168
7.2.1	Wake on LAN	170
7.2.2	Adapter Teaming	171
7.3	Lasst die Leitungen sich verbinden	172
7.3.1	Repeater.	173
7.3.2	Bridge	173
7.4	So funktionieren Switches	174
7.4.1	Methoden der Durchleitung	175
7.4.2	Spanning Tree Protocol	175
7.4.3	Managed Switches	177
7.5	Konvertieren und Verbinden	179
7.5.1	Medienkonverter.	179
7.5.2	Modems	181
7.5.3	Multiplexer	182
7.6	Router verbinden diese (Netzwerk-)Welt	183
7.7	Virtuelle Netzwerkkomponenten	185
7.8	Fragen zu diesem Kapitel	186
8	Der TCP/IP-Stack	189
8.1	Das Modell und die Praxis.	189
8.1.1	Vergleich OSI-Modell mit dem DOD-4-Modell	189
8.1.2	Der Aufbau der Adressierung	190
8.2	Die Grundlagen der IP-Adressierung.	193
8.2.1	CIDR statt Adressklassen.	196
8.2.2	Private Netzwerke unter IPv4	198
8.2.3	Ausnahmen und besondere Adressen	198
8.2.4	Der IPv4-Header.	198
8.3	IPv6	200
8.3.1	Der Header von IPv6	201
8.3.2	Spezielle Adressen unter IPv6.	202

8.4	Subnetztierung von Netzen	204
8.5	Von NAT bis uPnP	206
8.5.1	NAT und PAT	206
8.5.2	Universal Plug and Play	207
8.6	Weitere Protokolle auf dem IP-Layer	208
8.6.1	ICMP und IGMP	208
8.6.2	ARP	209
8.7	TCP und UDP	210
8.8	Die Geschichte mit den Ports	212
8.9	Fragen zu diesem Kapitel	214
9	Serverrollen	217
9.1	Dienste und Rollen	218
9.2	Datei- und Druckdienste	220
9.2.1	Dateidienste verwaltet der Fileserver	220
9.2.2	Printserver verwalten Drucker und ihre Aufträge	222
9.3	Internetdienste	224
9.3.1	Webserver	224
9.3.2	FTP-Server	227
9.4	Netzwerkdienste	228
9.4.1	DNS-Server	229
9.4.2	DHCP-Server	232
9.4.3	Zeitsynchronisations-Server	235
9.4.4	Überwachungsserver	236
9.4.5	Server mit Fernzugriff (RAS-Server)	237
9.4.6	VPN unter Linux	238
9.5	Messaging-Server (Mailserver)	240
9.5.1	Posteingangsdienste (Postfachzugriff)	240
9.5.2	Postausgangsdienst	241
9.5.3	Unix- und Linux-Mailserver	241
9.5.4	Die kommerziellen Server	242
9.5.5	Webmail	243
9.5.6	Cloud-Systeme	244
9.6	Sicherheits- und Authentifizierungsdienste	244
9.6.1	Domänen-Controller	244
9.6.2	Certificate Authorities (CA)	246
9.6.3	Rights-Management-Server	248
9.7	Anwendungsserver	248
9.7.1	Datenbankserver	249

9.7.2	Anwendungsserver.....	249
9.7.3	Anwendungsarchitekturen.....	250
9.8	Internet, Intranet und Extranet.....	251
9.9	Fragen zu diesem Kapitel.....	253
10	Übersicht zu Netzbetriebssystemen.....	255
10.1	Windows-Server von NT bis 2012.....	256
10.1.1	Historische Entwicklung.....	256
10.1.2	NT-Architektur.....	257
10.1.3	Unterschiedliche Editionen Server 2008.....	258
10.1.4	Unterschiedliche Editionen Server 2012.....	259
10.1.5	Windows Server 2008/R2.....	260
10.1.6	Windows Server 2012 und 2012 R2.....	262
10.1.7	Entscheidungshilfen.....	263
10.1.8	Sicherheitsfunktionen.....	264
10.2	*nix-Systeme.....	265
10.2.1	Linux.....	267
10.2.2	Einsatzgebiete.....	268
10.3	Fragen zu diesem Kapitel.....	270
11	Installation von Netzbetriebssystemen.....	273
11.1	Vorbereitungen für die Installation.....	273
11.1.1	Anforderungen.....	275
11.1.2	Dimensionierung.....	275
11.1.3	Serverplanung.....	275
11.2	Installation Microsoft Windows Server 2003.....	276
11.3	Installation Microsoft Windows Server 2008.....	278
11.3.1	Standardinstallation.....	279
11.3.2	Rollen und Features.....	282
11.3.3	Server 2008 Core-Installation.....	283
11.4	Installation Windows Server 2012 und 2012 R2.....	285
11.4.1	Schlusskonfiguration.....	285
11.4.2	Rollen und Features.....	286
11.4.3	Server Core.....	287
11.5	Automatisierungsstrategien.....	288
11.5.1	Die Bereitstellungsumgebung.....	288
11.5.2	Powershell Installation.....	291
11.5.3	Klonen virtueller Domänen-Controller.....	292
11.5.4	Beispiele.....	292

11.6	Unix/Linux-artige Betriebssysteme	294
11.6.1	Systemvoraussetzungen	294
11.6.2	Planung (Partitionierung)	295
11.6.3	Installation	297
11.6.4	Erste Schritte nach der Installation	305
11.6.5	Automatisierte Installationen	309
11.7	Fragen zu diesem Kapitel	313
12	Konfigurationsbetrachtungen.	315
12.1	Der Einfluss des Dateisystems	315
12.1.1	NTFS	316
12.1.2	Ext2/Ext3	321
12.1.3	Ext4	327
12.1.4	ReiserFS	327
12.1.5	XFS	328
12.1.6	ZFS	328
12.1.7	VMFS	329
12.2	Speicherplatzberechnung	329
12.2.1	Speicherplatz berechnen	330
12.2.2	Quotas unter Windows	331
12.2.3	Quotas unter Linux	331
12.3	Verzeichnisdienste	333
12.3.1	LDAP	333
12.3.2	NDS	334
12.3.3	AD DS – Active Directory Services	338
12.4	Gruppenrichtlinien (Group Policy Object, GPO)	342
12.5	Dateiübertragungsprotokolle	344
12.5.1	Das SMB-Protokoll	344
12.5.2	Samba	345
12.6	Fragen zu diesem Kapitel	348
13	Servermanagement	349
13.1	Remoteverbindungen	349
13.1.1	Telnet	350
13.1.2	SSH	352
13.1.3	VNC	355
13.1.4	RDP (Remote Desktop Protocol)	356
13.1.5	MSTSC (Remote Desktop-Client)	358
13.1.6	rdesktop (Linux)	360

13.2	Ereignisanzeige und Ereignisprotokoll	360
13.2.1	Das Ereignisprotokoll	360
13.2.2	Die Windows-Ereignisanzeige	361
13.3	Hardware-Monitoring	362
13.4	Baseline-Management	363
13.5	Leistungsüberwachung	364
13.5.1	Schlüsselwerte	365
13.5.2	Microsoft Performance-Monitor	366
13.5.3	Data Collector Sets/Performance-Logs	368
13.5.4	MRTG und RRDtool	370
13.6	SNMP	372
13.7	Web-Base Enterprise Management (WBEM)	374
13.8	Windows-Verwaltungsmechanismen	374
13.8.1	Windows Management Instrumentarium (WMI)	374
13.8.2	PowerShell	375
13.9	Hilfen	376
13.9.1	Manpages	377
13.9.2	GNU info und How-tos	378
13.9.3	Windows-Hilfe	378
13.9.4	Microsoft Knowledge Base	379
13.10	Fragen zu diesem Kapitel	379
14	Ein Server, viele Server, Wolke	381
14.1	Deployment-Szenarien	381
14.2	Virtualisierung	384
14.2.1	Hardwarevirtualisierung	384
14.2.2	Desktop-Virtualisierung	390
14.2.3	Anwendungsvirtualisierung	391
14.2.4	Storage-Virtualisierung	392
14.3	Cloud Computing	394
14.3.1	Cloud-Computing-Servicemodelle	394
14.3.2	Cloud-Computing-Betriebsmodelle	396
14.3.3	Beispiele von Clouds	396
14.3.4	SaaS ohne Ende	399
14.3.5	Es ist Ihre Wahl	399
14.4	Fragen zu diesem Kapitel	399
15	Physische Sicherheit für Ihre Server	401
15.1	Der sichere Serverraum	402
15.1.1	Wo kommt der Server hin	402

15.1.2	Rack oder Tower?	403
15.2	Klima, Strom und Umwelteinflüsse	404
15.2.1	Die Stromzufuhr	405
15.2.2	Klimafaktoren	405
15.2.3	Umwelteinflüsse	407
15.3	Zutrittskonzepte	408
15.3.1	Schlüsselsysteme	409
15.3.2	Badges und Keycards	410
15.3.3	Biometrische Erkennungssysteme	411
15.3.4	Zutrittsschleusen	412
15.3.5	Videoüberwachung	413
15.3.6	Multiple Systeme	414
15.4	Proaktiver Unterhalt	414
15.5	Monitoring	416
15.6	Fragen zu diesem Kapitel	416
16	Sicherheit und Unterhalt	419
16.1	Wer darf an den Server?	419
16.1.1	Authentifizierungsmethoden	419
16.1.2	RADIUS	420
16.1.3	TACACS, XTACACS und TACACS+	421
16.2	Zugriffsrechte auf Server und Systemen	422
16.2.1	Mandatory Access Control (MAC)	422
16.2.2	Discretionary Access Control (DAC)	423
16.2.3	Role Based Access Control (RBAC)	424
16.2.4	Principle of Least Privileges	426
16.3	Server gegen Angriffe schützen	426
16.3.1	Das System gegen Malware schützen	426
16.3.2	Netzwerksicherheitsmaßnahmen	427
16.3.3	Was leistet eine Firewall?	429
16.3.4	Regelwerke auf Firewalls	431
16.3.5	Das Konzept der DMZ	433
16.3.6	Intrusion Detection	434
16.4	Sichere Software: Vom Hotfix zum Upgrade	436
16.4.1	Problemkategorien	436
16.4.2	Maintenance-Produkte	437
16.5	Software nachinstallieren unter *nix	438
16.5.1	Kompilieren ab Sourcecode	438
16.5.2	Vorgefertigte Pakete	440

16.5.3	RPMs managen.	441
16.6	Software-Maintenance für Windows Server	442
16.6.1	Update- und Patch-Philosophie von Microsoft.	443
16.6.2	Microsoft-Update	444
16.6.3	Windows Update Service (WSUS).	445
16.6.4	Microsoft System Center	446
16.7	Fragen zu diesem Kapitel	447
17	Datensicherung ist nichts für Feiglinge.	449
17.1	Grundlagen der Datensicherungstechnologien.	449
17.1.1	DAT/DDS-Laufwerke.	453
17.1.2	AIT und S-AIT	455
17.1.3	VXA	456
17.1.4	DLT und SDLT	457
17.1.5	LTO/Ultrium.	459
17.1.6	RDX – Fast wie Band, aber Disk	461
17.1.7	Datensicherung auf Disks	463
17.2	Unterschiedliche Sicherungsziele	464
17.2.1	Externe Festplatten	464
17.2.2	DVD und Blu-ray im Server?	465
17.2.3	Das LAN-Backup.	465
17.2.4	Das hierarchische Speichermanagement	466
17.3	Das Datensicherungskonzept	467
17.4	Methoden der Datensicherung	471
17.4.1	Technische Verfahren	471
17.4.2	Imaging und Sicherung virtueller Umgebungen.	472
17.4.3	Organisatorische Methoden.	474
17.4.4	Die Onlinesicherung und -archivierung	475
17.5	Datensicherung in der Praxis	476
17.5.1	Windows-interne Datensicherung.	477
17.5.2	Standard Unix-Tools	478
17.5.3	Open-Source-Programme	480
17.5.4	Kommerzielle Sicherungsprogramme	481
17.6	Fragen zu diesem Kapitel	484
18	Disaster Recovery.	487
18.1	Übersicht zur Disaster Recovery-Planung	487
18.2	Analyse	489
18.2.1	Ausfallszenarien	489
18.2.2	Impact-Analyse	489

18.3	Umsetzung eines DRP	492
18.3.1	Strategie und Planung	492
18.3.2	Verschiedene Implementationsansätze	493
18.4	Disaster Recovery-Plan testen	495
18.5	Wartung des Disaster Recovery	496
18.5.1	Punktuelle Anpassungen	496
18.5.2	Regelmäßige Überprüfung	496
18.6	Merkmale zum Disaster Recovery	497
18.7	Fragen zu diesem Kapitel	497
19	Unterhalt und Support	499
19.1	Wie treten Sie auf?	499
19.2	Wie gehen Sie vor?	501
19.3	Fragen zu diesem Kapitel	504
20	Troubleshooting in der Praxis	507
20.1	Netzwerkfehlersuche	507
20.2	Programme zur Fehlersuche im Netzwerk	508
20.2.1	ipconfig	508
20.2.2	Ping	509
20.2.3	Routenverfolgungsprogramme	510
20.2.4	Nmap	513
20.2.5	nslookup	513
20.2.6	nbtstat	514
20.2.7	net use	515
20.3	Lokale Fehlersuche am Server	516
20.3.1	Vorbereitung	516
20.3.2	Startprobleme der Hardware	517
20.3.3	Start-Scripts als Problemquelle	518
20.4	Startprozess und Startprobleme	518
20.4.1	Die Übersicht über den Startprozess	518
20.4.2	Startprozess mit NTLDR	519
20.4.3	Startprozess mit BOOTMGR	519
20.5	Performance-Probleme	521
20.6	Dateisysteme	523
20.7	Datenträger – sicher halten, sicher löschen	524
20.7.1	Datenträger verschlüsseln	524
20.7.2	Sicheres Löschen	525
20.8	Fragen zu diesem Kapitel	526

21	Die CompTIA Server+-Prüfung	529
21.1	Was von Ihnen verlangt wird	530
21.2	Wie Sie sich vorbereiten können	530
21.3	Wie eine Prüfung aussieht	531
21.4	Beispielprüfung zu CompTIA Server+	535
A	Anhänge	559
A.1	Hier finden Sie die Prüfungsthemen.	559
A.2	Antworten auf den Vorbereitungstest	581
A.3	Antworten zu den Kapitelfragen.	582
A.4	Antworten zur Beispielprüfung	584
B	Abkürzungsverzeichnis	585
	Stichwortverzeichnis	595