

Inhaltsverzeichnis

Vorwort	13
Kapitel 1 Windows Server 2022 Essentials: Die Grundlagen	15
1.1 Windows Server 2022 Essentials richtig lizenzieren	16
1.1.1 Besonderheiten bei Windows Server 2022 Essentials	16
1.1.2 Windows Server 2022 Standard versus Essentials	17
1.1.3 Lizenz einschränkungen von Windows Server 2022 Essentials	17
1.1.4 Clientzugriffslizenzen beachten	18
1.2 Gebrauchte Server und Software günstig kaufen – auch als OEM	20
1.2.1 Auch gebrauchte Lizenzen können bares Geld sparen	21
1.2.2 Soft & Cloud: Gebrauchte Software aus der EU mit TÜV-Zertifizierung	22
1.2.3 OEM-Lizenzierung für Windows Server verstehen und Geld sparen	22
1.2.4 Direct OEM, Reseller Option Kit und Channel OEM für System Builder	23
1.2.5 Spezielle Lizenzbedingungen in Deutschland nutzen: Gebrauchte OEM-Lizenzen kaufen	24
1.3 Windows Server 2022 Essentials installieren und einrichten	25
1.4 Microsoft 365: Welches Abonnement ist am besten für Sie geeignet?	25
1.4.1 Microsoft 365 mit Word, Excel und PowerPoint	26
1.4.2 Unterschied zwischen Microsoft 365 und Microsoft Office 2021	26
1.4.3 Microsoft 365 für Profis und Unternehmen: E-Mail-Postfach, SharePoint, Teams und OneDrive	27
1.4.4 Microsoft Office für Unternehmen ohne Postfach, SharePoint und Teams	27
1.4.5 Microsoft Office plus Clouddienste in Microsoft 365 Business Standard und Premium	27
1.4.6 Maximale Sicherheit für KMU mit Microsoft 365 Business Premium	28
Kapitel 2 Windows Server 2022 Essentials installieren und einrichten	29
2.1 Das sollten Sie vor der Installation beachten	29
2.2 Neuinstallation von Windows Server 2022 Essentials	30
2.2.1 USB-Installationsstick erstellen	30
2.2.2 Windows Server 2022 Essentials installieren	33
2.3 Windows Server 2022 Essentials nach der Installation einrichten	38
2.3.1 Das richtige Netzwerkprofil einstellen	38
2.3.2 Grundlegende Einstellungen für Windows Server 2022 Essentials	39
2.3.3 Windows Server 2022 aktivieren	40
2.3.4 Treiberinstallation überprüfen	41
2.3.5 Firmware und BIOS/UEFI aktualisieren	41
2.3.6 Netzwerkverbindung testen	42
2.3.7 Windows Update aktivieren	42
2.3.8 Media Player deinstallieren	43
2.3.9 Computernamen und Domänenmitgliedschaft festlegen	44
2.3.10 Aktivieren von Remotedesktop in Windows Server 2022	45
2.3.11 Windows Server 2022 mit Windows 10/11 verwalten	46
2.4 Zusammenfassung	49

Kapitel 3	Erste Schritte mit Windows Server 2022 Essentials	51
3.1	Erste Schritte nach der Installation	51
3.1.1	Windows Server 2022 mit Windows 10/11 verwalten	52
3.2	Troubleshooting: Erweiterte Startoptionen nutzen	55
3.2.1	Starten der automatischen Reparatur von Windows Server 2022	56
3.2.2	Windows Server 2022 im abgesicherten Modus starten	57
3.2.3	Abgesicherter Modus über msconfig.exe	57
3.3	Serverrollen mit dem Best Practices Analyzer überprüfen	58
3.3.1	Überprüfen von Servern über das Netzwerk	59
3.3.2	BPA für Windows Server 2022 Essentials starten	60
3.3.3	BPA auswerten	61
3.4	Windows Admin Center in der Praxis	62
3.4.1	Admin Center-Gateway installieren und aktualisieren	63
3.4.2	Verbindungsaufbau zu Servern herstellen	64
3.4.3	Fehler bei der Verbindung beheben	65
3.4.4	Server im Windows Admin Center verwalten	66
3.4.5	Datei-Explorer, Registry-Editor, PowerShell und Remotedesktop nutzen	67
3.4.6	Gatewayzugriff steuern	68
3.4.7	Zertifikat für das Windows Admin Center steuern	69
3.4.8	Erweiterungen für das Windows Admin Center	69
3.4.9	Windows Admin Center und Microsoft Azure	70
3.5	Azure Arc: Server über das Internet remote verwalten	73
3.5.1	Kostenlose Anbindung lokaler Server	73
3.5.2	Lokal angebundene Server in Azure Arc verwalten	75
3.5.3	Remotedesktopverbindung zum Server über das Internet	79
3.5.4	Sicherheits- und Updatecheck des Servers über das Windows Admin Center	80
3.6	OpenVPN, Pritunl, WireGuard, SoftEther: VPNs mit Open Source	81
3.6.1	OpenVPN – seit Jahren etabliert und in vielen Geräten enthalten	82
3.6.2	WireGuard – der Platzhirsch beim Aufbau von VPNs	82
3.6.3	Pritunl: VPNs mit IPsec, OpenVPN und WireGuard	85
3.6.4	SoftEther: Open Source-VPN-Server für Windows, Linux, macOS, Solaris und FreeBSD	86
3.6.5	Algo VPN: Das VPN mit Ansible-Skriptss und WireGuard oder IPsec	86
3.7	Zusammenfassung	87
Kapitel 4	Active Directory	89
4.1	Active Directory für Einsteiger	89
4.1.1	Das ist Active Directory	90
4.1.2	Konkreter Nutzen eines Active Directory	90
4.1.3	Tipps für die Verwaltung von Active Directory in kleinen Unternehmen	91
4.1.4	Für Sicherheitsgruppen und Server eine eigene OU erstellen	92
4.1.5	Standardisierte Namenskonventionen nutzen	92
4.1.6	Active Directory überwachen	93
4.2	DNS für Active Directory installieren	93
4.2.1	Vorbereitungen für DNS treffen und DNS installieren	94
4.2.2	Erstellen der notwendigen DNS-Zonen für Active Directory	96
4.2.3	Überprüfung und Fehlerbehebung der DNS-Einstellungen	100
4.2.4	Namensauflösung zum Internet konfigurieren	101
4.3	Installation der Active Directory-Domänenrolle	103
4.3.1	Starten der Einrichtung von Active Directory	104
4.3.2	Administratorkonto umbenennen	109

4.3.3	DNS in Active Directory integrieren und sichere Updates konfigurieren	109
4.3.4	DNS-IP-Einstellungen anpassen	110
4.4	Problembehandlung bei der Bereitstellung von Domänencontrollern	111
4.4.1	Einstieg in das Troubleshooting mit Active Directory	111
4.4.2	Diese fünf Fehler verursachen die meisten Probleme	112
4.4.3	Protokolldateien auswerten	112
4.4.4	NetTools: Portable Toolsammlung für Troubleshooting in Active Directory	113
4.5	Das Active Directory-Verwaltungszentrum	115
4.5.1	Objekte schützen und wiederherstellen	116
4.6	Verwaltungs-PCs für Administratoren einrichten	118
4.6.1	RDP-Verbindung und DNS konfigurieren	118
4.6.2	DNS-Auflösung auf Admin-PC sicherstellen	118
4.6.3	RDP-Verbindung auf Arbeitsstationen herstellen	118
4.7	Arbeitsstationen in die Domäne aufnehmen	121
4.7.1	IP-Einstellungen vor der Domänenaufnahme konfigurieren	121
4.7.2	Grundlagen für die Aufnahme in Active Directory konfigurieren	122
4.7.3	Computer über Assistenten in Active Directory aufnehmen	123
4.8	Kennwortsicherheit in Active Directory	125
4.8.1	Kennwörter und Richtlinien im Windows Admin Center verwalten	125
4.8.2	Kostenloses Tool: Specops Password Auditor	126
4.8.3	Kennwortrichtlinien in Active Directory nutzen	127
4.9	Zusammenfassung	129
Kapitel 5	Benutzer und Gruppen verwalten	131
5.1	Einstieg in die Verwaltung von Benutzern	131
5.2	Grundlagen zur Verwaltung von Benutzern	132
5.2.1	Active Directory-Benutzerverwaltung	133
5.2.2	Verwalten von Benutzerkonten	135
5.3	Benutzerprofile verstehen und nutzen	138
5.3.1	Benutzerprofile lokal und im Profieinsatz	138
5.3.2	Ordnerumleitungen von Profilen	140
5.4	Anmelde- und Abmeldeskripts für Benutzer und Computer	142
5.5	Gruppen verwalten	144
5.5.1	Gruppen anlegen und verwenden	144
5.5.2	Berechtigungen für Benutzer und Gruppen verwalten	146
5.6	Zusammenfassung	148
Kapitel 6	Datenträger und Datenspeicherung verwalten	149
6.1	Datenträger erstellen und anpassen	149
6.1.1	Einrichten von Datenträgern	151
6.1.2	Konfigurieren von Laufwerken	155
6.1.3	Komprimieren von Datenträgern und Ordnern	157
6.1.4	Festplattenverwaltung in der PowerShell und Befehlszeile	158
6.1.5	Repair-Cmdlets für das Troubleshooting von SSD/HDD nutzen	159
6.2	Mit GPT-Partitionen und ReFS arbeiten	161
6.2.1	GPT versus MBR	161
6.2.2	Verkleinern und Erweitern von Datenträgern	162
6.2.3	ReFS nutzen	164
6.3	Verwalten von Datenträgern	165
6.3.1	Defragmentierung verwalten	166
6.3.2	Hardware und Richtlinie von Datenträgern verwalten	167

6.4	BitLocker-Laufwerkverschlüsselung	169
6.4.1	Grundlagen zu BitLocker und Trusted Platform Module (TPM)	170
6.4.2	BitLocker schnell und einfach aktivieren	171
6.4.3	Troubleshooting für BitLocker	173
6.5	Verwenden von Schattenkopien	174
6.6	Zusammenfassung	176
Kapitel 7	Ordner freigeben und Berechtigungen steuern	177
7.1	Ordnerfreigaben richtig planen und durchführen	178
7.1.1	Sinnvolle Freigaben	178
7.1.2	Benutzer und Organisationseinheiten anlegen	179
7.2	Gruppen anlegen und Ordner freigeben	181
7.2.1	Ordner freigeben	183
7.2.2	Berechtigungen im Dateisystem	184
7.2.3	Besitzer für ein Objekt festlegen	187
7.2.4	Der Assistent zum Erstellen von Freigaben	187
7.3	Freigaben verwalten, verbinden und Offlinedateien nutzen	189
7.3.1	Anzeigen aller Freigaben	190
7.3.2	Auf Freigaben über das Netzwerk zugreifen	191
7.3.3	Freigaben im Windows Admin Center verwalten	192
7.3.4	Offlinedateien für den mobilen Einsatz unter Windows 10/11	193
7.4	Datenaustausch zwischen macOS und Windows: Hybride Freigaben nutzen	199
7.4.1	Freigaben in macOS erstellen und in Windows oder Linux nutzen	199
7.4.2	Von Windows aus auf Freigaben in macOS zugreifen	200
7.4.3	Vom Mac aus auf Windows-Freigaben zugreifen	201
7.5	Zusammenfassung	201
Kapitel 8	Datensicherung und Schutz vor Ransomware	203
8.1	Datensicherungsstrategien und -lösungen	203
8.1.1	Backup in die Cloud	204
8.2	Grundlagen zur Datensicherung	206
8.3	Windows Server-Sicherung installieren und konfigurieren	207
8.3.1	Datensicherung in Windows Server 2022 einrichten	207
8.3.2	Sicherung in der Eingabeaufforderung und PowerShell konfigurieren	214
8.4	Daten mit dem Sicherungsprogramm wiederherstellen	215
8.4.1	Einzelne Dateien mit dem Sicherungsprogramm wiederherstellen	215
8.4.2	Kompletten Server mit dem Sicherungsprogramm wiederherstellen	218
8.5	Erweiterte Wiederherstellungsmöglichkeiten	220
8.5.1	Schrittaufzeichnung – Fehler in Windows nachvollziehen und beheben	220
8.5.2	Datensicherung über Ereignisanzeige starten	221
8.6	Windows-Abstürze analysieren und beheben	222
8.6.1	Bluescreens im Griff behalten	223
8.6.2	Microsoft Windows File Recovery Tool	226
8.7	Azure Backup	229
8.7.1	Windows Server-Sicherung und Azure Backup: Das perfekte Team gegen Ransomware	230
8.7.2	Windows Admin Center nutzen	230
8.7.3	Windows Admin Center mit dem Server verbinden	231
8.7.4	Windows Admin Center kostenlos bei Azure registrieren	232
8.7.5	Azure Backup einrichten	233
8.7.6	Manuelle Einrichtung und Verwaltung von Azure Backup	234

8.7.7	Sicherungsplan für die Datensicherung zu Azure Backup erstellen	238
8.7.8	Daten mit Azure Backup wiederherstellen	240
8.8	Windows 11 richtig mit Bordmitteln sichern	242
8.8.1	Imagesicherung mit Windows 11 durchführen: Betriebssystem und Anwendungen sichern	242
8.8.2	Systemwiederherstellung und Wiederherstellungspunkte aktivieren	243
8.9	Zusammenfassung	243
Kapitel 9	Schutz vor Ransomware und Malware mit Bordmitteln erreichen	245
9.1	Microsoft Defender gegen Malware	245
9.2	Microsoft Defender richtig konfigurieren	246
9.2.1	Windows-Sicherheit: der Viren- und Bedrohungsschutz	246
9.2.2	Ransomware-Schutz nutzen	249
9.2.3	Scanoptionen in Microsoft Defender steuern und Scans durchführen	249
9.2.4	Kernisolierung und andere Sicherheitsfunktionen aktivieren	250
9.3	Sysinternals Process Explorer	251
9.3.1	Virensuche mit Process Explorer	251
9.3.2	Prozesse nach Viren scannen	252
9.4	Secured-Core-Funktionen auf dem Server aktivieren	255
9.4.1	Secured-Core für ein sicheres Netzwerk	255
9.4.2	Secured-Core-Server und das Windows Admin Center	256
9.4.3	Secured-Core-Funktionen überprüfen und konfigurieren	256
9.4.4	Secured-Core setzt auf Virtualization Based Security	257
9.5	Microsoft Defender for Business	257
9.5.1	Benutzer und Geräte an Microsoft 365 for Business anbinden	258
9.5.2	Geräte von Anwendern an Microsoft Defender for Business anbinden	260
9.5.3	Erfolgreiche Anbindung an Microsoft Defender for Business testen	261
9.6	Active Directory auf dem Server absichern mit Tipps von PingCastle	261
9.6.1	Domäne mit PingCastle scannen	261
9.7	Windows Defender Firewall nutzen	264
9.7.1	Windows Defender-Firewall mit Gruppenrichtlinien steuern	265
9.7.2	Firewallregeln für SQL-Server in der grafischen Oberfläche erstellen	265
9.8	Die Sicherheit der Firewall über das Internet testen und tunen	267
9.8.1	GeoIP-Filter und Blockierlisten	267
9.8.2	Geöffnete Ports schließen	268
9.8.3	ShieldsUP und Co helfen beim Testen der eigenen Firewall	269
9.8.4	Mit Portchecker.de einzelne Ports testen	269
9.8.5	Diagnose der eigenen Firewall überprüfen	269
9.9	Zusammenfassung	270
Kapitel 10	Gruppenrichtlinien	271
10.1	Erste Schritte mit Richtlinien	271
10.1.1	Verwaltungswerkzeuge für Gruppenrichtlinien	272
10.1.2	Wichtige Begriffe für Gruppenrichtlinien	272
10.1.3	Aktuelle Gruppenrichtlinienvorlagen für Windows und Office hinterlegen	275
10.1.4	Gruppenrichtlinien für Windows 11 22H2 und neuer	275
10.1.5	Gruppenrichtlinien für Office 2016/2019/2021 und Microsoft 365	276
10.1.6	Gruppenrichtlinien für Microsoft Edge, Google Chrome und Mozilla Firefox ...	276
10.2	Gruppenrichtlinien verstehen und verwalten	278
10.2.1	Neue Gruppenrichtlinie erstellen	278
10.2.2	GPO mit einem Container verknüpfen	279

10.2.3	Gruppenrichtlinien erzwingen und Priorität erhöhen	281
10.2.4	Vererbung für Gruppenrichtlinien deaktivieren	284
10.3	Sicherheitseinstellungen in Windows	285
10.3.1	Sicherheitsvorlagen bei Microsoft herunterladen	285
10.3.2	Vorlagen von Microsoft in eigene Richtlinien importieren	286
10.3.3	Windows Server 2022 Essentials mit Richtlinien absichern	288
10.3.4	Datenschutz bei Windows 11 verbessern	290
10.3.5	Microsoft Store, Cortana und Datensammlungen in Windows 10/11 sperren	293
10.3.6	Sicherheitseinstellungen für das Netzwerk steuern	294
10.3.7	Überwachter Ordnerzugriff – Schutz vor Ransomware	294
10.3.8	Firewalleinstellungen über Gruppenrichtlinien setzen	296
10.4	Benutzer und Kennwörter mit Gruppenrichtlinien absichern	296
10.4.1	Mit Lithnet Password Protect und Filtern Kennwörter in Active Directory schützen	298
10.5	Gruppenrichtlinien testen und Fehler beheben	300
10.5.1	Einstieg in die Fehlerbehebung von Gruppenrichtlinien	301
10.5.2	Vorgehensweise bei der Fehlerbehebung von Gruppenrichtlinien	301
10.5.3	Policy Analyzer zur Fehlerbehebung nutzen	302
10.5.4	Datensicherung und Wiederherstellung von Gruppenrichtlinien	303
10.5.5	Gruppenrichtlinien mit der PowerShell sichern und wiederherstellen	306
10.6	Sicherheit in Office 2016/2019 und Office 2021 mit GPOs einstellen	307
10.6.1	Sicherheit in Office 2021 einstellen mit GPOs und automatische Bereitstellung ..	308
10.6.2	Gemeinsames Bearbeiten von Dokumenten aktivieren	308
10.6.3	Click-To-Run-Installer	309
10.6.4	Office 2021 automatisiert installieren und konfigurieren	309
10.6.5	Gruppenrichtlinien für Office 2016/2019/2021 und Microsoft 365	311
10.6.6	Makros mit Richtlinien steuern	312
10.6.7	Office 2021 aktualisieren	314
10.7	Zusammenfassung	315

Kapitel 11 Windows-Updates automatisieren 317

11.1	Update-Steuerung in Windows 11	317
11.1.1	Windows-Updates mit der Einstellungs-App konfigurieren	318
11.1.2	Updates deinstallieren	319
11.2	Rollback von Windows 11 auf Windows 10 oder zu älterer Windows 11-Version	320
11.2.1	Windows 11 updaten	320
11.2.2	Windows 11 zurücksetzen	321
11.2.3	Windows 11 über Computerreparaturoptionen wiederherstellen	322
11.2.4	Update zu Windows 11 rückgängig machen	323
11.3	Gruppenrichtlinieneinstellungen für Windows-Updates richtig setzen	325
11.3.1	Automatische Updates konfigurieren	326
11.3.2	Probleme bei der Installation von Updates beheben	327
11.4	Zusammenfassung	327

Kapitel 12 Überwachung und Fehlerbehebung 329

12.1	Fehlerbehebung in Windows Server – Ereignisanzeige	329
12.1.1	Ereignisanzeige nutzen	329
12.2	Überwachung der Systemleistung	334
12.2.1	Die Leistungsüberwachung	335
12.2.2	Indikatorendaten in der Leistungsüberwachung beobachten	337
12.2.3	Sammlungssätze nutzen	338

12.2.4	Speicherengpässe beheben	338
12.2.5	Prozessorauslastung messen und optimieren	340
12.2.6	Der Task-Manager als Analysewerkzeug	341
12.2.7	Laufwerke und Datenträger überwachen – Leistungsüberwachung und Zusatztools	342
12.3	Aufgabenplanung – Windows automatisieren	343
12.3.1	Aufgabenplanung verstehen	344
12.3.2	Erstellen einer neuen Aufgabe	347
12.4	Prozesse und Dienste überwachen	348
12.4.1	Dienste in der PowerShell verwalten	349
12.4.2	Dateisystem, Registry und Prozesse überwachen – Sysinternals Process Monitor ...	353
12.4.3	Laufende Prozesse analysieren – Process Explorer	356
12.4.4	Wichtige Informationen immer im Blick – BgInfo	360
12.4.5	Systeminformationen in der Eingabeaufforderung anzeigen – PsInfo	362
12.5	Zusammenfassung	363
Kapitel 13	Netzwerkeinstellungen, DHCP und Infrastruktur	365
13.1	Grundlagen zur Netzwerkanbindung	365
13.1.1	Anbindung des Computers an das Netzwerk	366
13.1.2	Erweiterte Verwaltung der Netzwerkverbindungen	367
13.1.3	Eigenschaften von Netzwerkverbindungen und ihre erweiterte Verwaltung	368
13.1.4	Eigenschaften von TCP/IP und DHCP	369
13.1.5	Routen verfolgen in der Eingabeaufforderung – Pathping und Tracert	372
13.2	Mit der PowerShell Netzwerkprobleme lösen	373
13.2.1	Get-NetIPAddress und Get-NetIPConfiguration	373
13.2.2	Test-NetConnection: Routen nachverfolgen und Verbindungen überprüfen	373
13.2.3	Get-NetTCPConnection: Ports und TCP-Verbindungen testen	374
13.3	Netzwerkeinstellungen für Active Directory	374
13.3.1	Netzwerkeinstellungen für die Domänenaufnahme konfigurieren	375
13.3.2	Domänenaufnahme durchführen	375
13.3.3	Domänenaufnahme testen	375
13.4	DHCP-Server einsetzen	379
13.4.1	Installation eines DHCP-Servers	379
13.4.2	Grundkonfiguration eines DHCP-Servers	380
13.4.3	DHCP-Server mit Tools testen und Fehler finden	387
13.4.4	DHCP-Verkehr mit WireShark überprüfen	388
13.4.5	Migration – Verschieben einer DHCP-Datenbank auf einen anderen Server	389
13.5	Zusammenfassung	390
Index		391