

PRAXISHANDBUCH · AUSGABE 2026

Windows Server Administration

LESEPROBE

Das Praxishandbuch für Systemadministratoren

Active Directory · DNS · DHCP · Netzwerk · Gruppenrichtlinien · Security · PKI · Hyper-V ·
Cluster · PowerShell · Troubleshooting

15 Kapitel · **Praxislabore** mit Schritt-für-Schritt-Ablauf · **Troubleshooting** in jedem Kapitel

Manfred Urbanetz

Rechtliches

Windows Server Administration – Das Praxishandbuch für Systemadministratoren

Ausgabe 2026

© 2026 Manfred Urbanetz. Alle Rechte vorbehalten.

Dieses Werk ist urheberrechtlich geschützt und für die persönliche Nutzung des Erwerbers lizenziert. Weitergabe, Vervielfältigung oder Veröffentlichung – auch auszugsweise – sind ohne schriftliche Genehmigung des Autors nicht gestattet.

Haftungsausschluss. Alle Anleitungen, Befehle und Skripte wurden für eine Lab-Umgebung geschrieben. Bitte teste jede Änderung zuerst in einer Testumgebung und sichere Produktivsysteme vor Eingriffen. Der Autor übernimmt keine Haftung für Schäden, die aus der Anwendung der beschriebenen Verfahren entstehen.

Marken. Microsoft, Windows, Windows Server, Active Directory, Hyper-V und PowerShell sind Marken der Microsoft Corporation. Dieses Buch steht in keiner Verbindung zu Microsoft und wird von Microsoft nicht unterstützt. Alle übrigen genannten Produkt- und Firmennamen sind Eigentum der jeweiligen Inhaber.

Über den Autor. Manfred Urbanetz ist Trainer und Kursentwickler (WIFI Innsbruck) für Windows Server und Netzwerke und arbeitet in der IT-Praxis mit Active Directory, Hyper-V und Security-Monitoring.

Inhaltsverzeichnis

Vorwort und Arbeitsweise	9
Die Lab-Umgebung	11
Teil I – Active Directory und Netzwerkgrundlagen	
Kapitel 1	Active Directory 13
Kapitel 2	AD-Replikation, Sites und Services 28
Kapitel 3	FSMO-Rollen und AD-Betrieb 40
Kapitel 4	DNS für Active Directory 52
Kapitel 5	DHCP im Unternehmenseinsatz 64
Kapitel 6	IP-Netzwerke und Routing 75
Teil II – Betrieb, Verwaltung und Sicherheit	
Kapitel 7	Gruppenrichtlinien – tiefgehend 88
Kapitel 8	Fileserver und Berechtigungsdesign 100
Kapitel 9	Windows Server Security 110
Kapitel 10	Kerberos und Authentifizierung 121
Kapitel 11	PKI mit Active Directory Certificate Services 130
Teil III – Virtualisierung und Hochverfügbarkeit	
Kapitel 12	Hyper-V 146
Kapitel 13	Failover Clustering 157
Teil IV – Automatisierung und Fehlersuche	
Kapitel 14	PowerShell für Administratoren 168
Kapitel 15	Troubleshooting-Methodik 181

Ausführliches Inhaltsverzeichnis

Kapitel 1 – Active Directory	13	2.19 Netzwerkabhängigkeiten der AD-Replikation	35
1.1 Lernziele und Kursziel	13	2.20 Troubleshooting – ein reproduzierbarer Ablauf	35
1.2 Lab-Topologie	13	2.21 Typische Fehlerbilder	35
1.3 Was Active Directory eigentlich ist	14	2.22 Praxislabor A – funktionierende Replikation beobachten	
1.4 Logische AD-Architektur	15	2.23 Praxislabor B – Standorterkennung prüfen	36 36
1.5 Physische Komponenten eines Domain Controllers	16	2.24 Praxislabor C – bewusstes Replikationsproblem	36
1.6 Warum DNS für Active Directory unverzichtbar ist	17	2.25 Konflikte und Last Writer – nur so tief wie nötig	37
1.7 DC Locator – wie ein Client seinen Domain Controller findet	18	2.26 Tombstones und gelöschte Objekte – Überblick	37
1.8 Global Catalog	19	2.27 Linging Objects – Konzept	37
1.9 Installation von DC01 – Planung und Voraussetzungen	19	2.28 Betriebscheck – was ein Administrator regelmäßig kontrolliert	37
1.10 DC01 als neue Gesamtstruktur installieren	20	2.29 Fachgespräch – typische Fragen und kurze Antworten	38
1.11 DC01 nach der Promotion prüfen	20	2.30 Schnellreferenz	39
1.12 DC02 als zusätzlichen Domain Controller installieren	21	Kapitel 3 – FSMO-Rollen und AD-Betrieb	40
1.13 Was nach DC02 technisch passiert	22	3.1 Lernziele	40
1.14 Sites, Subnetze und DC-Auswahl	23	3.2 Warum gibt es FSMO-Rollen?	40
1.15 Troubleshooting – systematisch statt zufällig	23	3.3 Überblick über die fünf FSMO-Rollen	41
1.16 Betriebschecks für Administratoren	24	3.4 Forest-weite Rollen	41
1.17 Architekturfragen – warum so und nicht anders?	24	3.5 Domänenweite Rollen	42
1.18 Was wir bewusst noch nicht vertiefen	25	3.6 PDC Emulator und Zeitdienst	43
1.19 Praxislabor	25	3.7 Infrastructure Master	43
1.20 Fachgespräch – typische Fragen	25	3.8 Rolleninhaber ermitteln	44
1.21 Abschlusscheckliste	26	3.9 Geplanter Transfer von FSMO-Rollen	44
1.22 Schnellreferenz – wichtigste Befehle	27	3.10 GUI-Werkzeuge für FSMO-Rollen	45
Kapitel 2 – AD-Replikation, Sites und Services	28	3.11 Seize – erzwungene Übernahme	45
2.1 Lernziele und Einordnung	28	3.12 Auswirkungen eines FSMO-Ausfalls	46
2.2 Wie AD-Replikation grundsätzlich funktioniert	28	3.13 Ausfallszenario: DC01 fällt dauerhaft aus	46
2.3 Welche Daten replizieren?	29	3.14 Forced Demotion	47
2.4 Active Directory Sites – warum sie wichtig sind	29	3.15 Metadata Cleanup	47
2.5 Step by Step – Sites und Subnetze anlegen	30	3.16 Der alte DC nach einem Seize	48
2.6 Intra-Site-Replikation	30	3.17 Betriebscheck für FSMO und DC-Gesundheit	48
2.7 Inter-Site-Replikation	31	3.18 Praxislabor 1 – Rollen kontrolliert verschieben	48
2.8 KCC – Knowledge Consistency Checker	31	3.19 Praxislabor 2 – Ausfallentscheidung simulieren	49
2.9 ISTG – Inter-Site Topology Generator	31	3.20 Typische Fehlerbilder	49
2.10 Site Links – die logischen WAN-Verbindungen	32	3.21 Fachgespräch – typische Fragen	50
2.11 Step by Step – Site Link konfigurieren	32	3.22 Schnellreferenz	50
2.12 Beispiel mit drei Standorten und Kosten	32	3.23 Abschlusscheckliste	51
2.13 Site Link Bridges – nur konzeptionell	33	Kapitel 4 – DNS für Active Directory	52
2.14 Replikationsmetadaten – was AD intern bewertet	33	4.1 Lernziele	52
2.15 Up-to-Date Vector und High-Watermark – Grundidee	33	4.2 Warum DNS für Active Directory so wichtig ist	52
2.16 repadmin – wichtigstes Werkzeug für AD-Replikation	34	4.3 DNS-Zonentypen im Überblick	53
2.17 dcdiag und PowerShell	34	4.4 AD-integrierte Zonen	53
2.18 Ereignisprotokolle	34	4.5 DomainDNSZones und ForestDNSZones	53

4.6 Die Zone _msdcs	54	5.25 Praxislabor B – DHCP Failover	72
4.7 SRV-Records verstehen	54	5.26 Praxislabor C – Fehlerdiagnose	73
4.8 DC Locator und DNS	55	5.27 Fachgespräch – typische Fragen	73
4.9 Dynamische DNS-Updates	55	5.28 Schnellreferenz	74
4.10 Forwarder und Root Hints	56	5.29 Abschlusscheckliste	74
4.11 Conditional Forwarder	56		
4.12 Delegation	57	Kapitel 6 – IP-Netzwerke und Routing	75
4.13 Stub Zone vs. Secondary Zone	57	6.1 Lernziele	75
4.14 Zone Transfers: AXFR, IXFR und Notify	57	6.2 Die Lab-Topologie	75
4.15 Reverse Lookup Zones	58	6.3 IPv4 wirklich verstehen	76
4.16 Aging und Scavenging	58	6.4 CIDR und gängige Masken	76
4.17 DNS Cache und negative Antworten	58	6.5 Subnetting: ein Netz in gleich große Teile zerlegen	77
4.18 DNS-Diagnosewerkzeuge	59	6.6 VLSM – unterschiedlich große Subnetze planen	77
4.19 Systematisches DNS-Troubleshooting	59	6.7 Wann liegt ein Ziel im eigenen Subnetz?	78
4.20 Typische Fehlerbilder	60	6.8 ARP – IP-Adresse zur MAC-Adresse auflösen	78
4.21 Praxislabor A – AD-DNS analysieren	60	6.9 Routing – wie entscheidet Windows?	79
4.22 Praxislabor B – Conditional Forwarder	60	6.10 Default Gateway und Default Route	79
4.23 Praxislabor C – Fehler: DC wird nicht gefunden	61	6.11 Statische Routen unter Windows	80
4.24 Praxislabor D – Fehlender SRV-Record	61	6.12 Metriken – wenn mehrere gleich spezifische Wege existieren	80
4.25 DNS und Active Directory – Betriebscheck	62	6.13 Paketweg durch einen Router	80
4.26 Fachgespräch – typische Fragen	62	6.14 ICMP – Diagnose und Fehlermeldungen	81
4.27 Schnellreferenz	62	6.15 MTU und Fragmentierung	81
4.28 Abschlusscheckliste	63	6.16 NAT – Adressen übersetzen	82
Kapitel 5 – DHCP im Unternehmenseinsatz	64	6.17 VLAN-Grundlagen für Administratoren	82
5.1 Lernziele	64	6.18 Windows RRAS als IPv4-Router	82
5.2 DHCP-Grundprinzip und DORA	64	6.19 Routing zwischen unseren beiden Netzen testen	83
5.3 Lease-Lifecycle	65	6.20 systematisches Routing-Troubleshooting	83
5.4 Scope-Planung	65	6.21 Typische Fehlerbilder	84
5.5 Scope, Exclusion und Reservation	66	6.22 Praxislabor A – Subnetting und VLSM	84
5.6 DHCP-Optionen	66	6.23 Praxislabor B – Windows Routing	84
5.7 DHCP in Active Directory autorisieren	66	6.24 Praxislabor C – Fehler gezielt erzeugen	85
5.8 DHCP Relay / IP Helper	67	6.25 Fachgespräch – typische Fragen	85
5.9 Superscope	67	6.26 Schnellreferenz	85
5.10 DHCP Policies	67	6.27 Abschlusscheckliste	86
5.11 Vendor Classes und User Classes	68		
5.12 DHCP und DNS-Dynamik	68	Kapitel 7 – Gruppenrichtlinien – tiefgehend	88
5.13 DHCP Failover – Konzept	69	7.1 Lernziele	88
5.14 Load Balance vs. Hot Standby	69	7.2 Was ist eine Gruppenrichtlinie technisch?	88
5.15 MCLT – Maximum Client Lead Time	69	7.3 GPC und GPT – zwei Replikationswege	89
5.16 Failover einrichten	69	7.4 GPO-Versionen und Konsistenz	89
5.17 Failover-Zustände verstehen	70	7.5 Wo können GPOs verknüpft werden?	89
5.18 Split Scope – historische Einordnung	70	7.6 LSDOU – Reihenfolge der Verarbeitung	90
5.19 PowerShell – wichtige Verwaltungsbefehle	71	7.7 Vererbung, Link Order und Priorität	90
5.20 Backup und Restore der DHCP-Konfiguration	71	7.8 Block Inheritance und Enforced	90
5.21 Relevante Eventlogs	71	7.9 Security Filtering – wer darf die GPO anwenden?	91
5.22 Systematisches DHCP-Troubleshooting	71	7.10 Authenticated Users – häufig missverstanden	91
5.23 Typische Fehlerbilder	72	7.11 WMI Filtering	91
5.24 Praxislabor A – Basis-DHCP für Clientnetz	72	7.12 Computer Configuration vs. User Configuration	92
		7.13 Loopback Processing	92

7.14 Group Policy Preferences (GPP)	92	Kapitel 9 – Windows Server Security	110
7.15 Item-Level Targeting	93	9.1 Lernziele	110
7.16 Praxisbeispiel – Laufwerke mit einer GPO	93	9.2 Sicherheitsmodell: mehrere Schutzschichten	110
7.17 Administrative Templates, ADMX und ADML	94	9.3 Windows Defender Firewall	111
7.18 Central Store	94	9.4 Eigene Firewall-Regel – Beispiel	111
7.19 Background Refresh und gpupdate	94	9.5 Microsoft Defender Antivirus	111
7.20 Resultant Set of Policy – was wirkt tatsächlich?	95	9.6 Windows LAPS	112
7.21 Group Policy Operational Eventlog	95	9.7 Windows LAPS – grober Ablauf	112
7.22 Abhängigkeiten: DNS, Kerberos, LDAP und SYSVOL	95	9.8 Privilegierte Konten trennen	113
7.23 Systematisches GPO-Troubleshooting	96	9.9 Protected Users	113
7.24 Typische Fehlerbilder	96	9.10 Credential Guard	113
7.25 Praxislabor A – Vererbung sichtbar machen	97	9.11 Service Accounts – warum klassische Konten problematisch sind	114
7.26 Praxislabor B – Security Filtering und WMI	97	9.12 gMSA – Group Managed Service Account	114
7.27 Praxislabor C – Loopback auf RDS	97	9.13 Rechte für Dienstkonto minimieren	114
7.28 Praxislabor D – Fehlerdiagnose	97	9.14 Advanced Audit Policy	115
7.29 PowerShell für GPO-Administratoren	98	9.15 Wichtige Security Event IDs	115
7.30 Fachgespräch – typische Fragen	98	9.16 Logon Types – wichtig für die Analyse	116
7.31 Schnellreferenz	98	9.17 Eventlog-Größen und zentrale Sammlung	116
7.32 Abschlusscheckliste	99	9.18 Administrative Baseline – Beispiel	116
Kapitel 8 – Fileserver und Berechtigungsdesign	100	9.19 Praxislabor A – Firewall und Defender	117
8.1 Lernziele	100	9.20 Praxislabor B – Windows LAPS	117
8.2 Architektur eines Windows-Fileservers	100	9.21 Praxislabor C – gMSA	117
8.3 Share Permissions vs. NTFS Permissions	101	9.22 Praxislabor D – Auditing	118
8.4 NTFS-Berechtigungen im Detail	101	9.23 Troubleshooting – systematischer Ablauf	118
8.5 Vererbung, explizite Rechte und Deny	101	9.24 Typische Fehlkonfigurationen	118
8.6 AGDLP und AGUDLP	102	9.25 PowerShell-Schnellreferenz	119
8.7 Beispiel: Abteilungsstruktur	102	9.26 Fachgespräch – typische Fragen	119
8.8 Root-Freigabe richtig aufbauen	102	9.27 Abschlusscheckliste	119
8.9 Access-Based Enumeration (ABE)	103	Kapitel 10 – Kerberos und Authentifizierung	121
8.10 Effective Access und Troubleshooting von ACLs	103	10.1 Lernziele	121
8.11 Typische Berechtigungsfehler	104	10.2 Kerberos im Active Directory	121
8.12 FSRM – File Server Resource Manager	104	10.3 Der Kerberos-Anmeldeablauf	122
8.13 Quotas und File Screening	104	10.4 Was befindet sich im Ticket?	122
8.14 Shadow Copies / Previous Versions	104	10.5 SPN – Service Principal Name	123
8.15 SMB – Versionen und Sicherheitsfunktionen	105	10.6 Kerberos oder NTLM?	123
8.16 SMB Signing und SMB Encryption	105	10.7 klist – Tickets sichtbar machen	124
8.17 DFS Namespace (DFSN)	105	10.8 Zeit und Clock Skew	124
8.18 DFS Replication (DFSR)	106	10.9 Der Double-Hop	124
8.19 DFSR – wichtige Betriebsaspekte	106	10.10 Delegation	125
8.20 PowerShell für Fileserver-Administratoren	106	10.11 Protokolltransition / S4U	125
8.21 Praxislabor 1 – Berechtigungsmodell sauber aufbauen	107	10.12 Namensauflösung und SPN-Namen	125
8.22 Praxislabor 2 – Fehler gezielt erzeugen	107	10.13 Typische Kerberos-Fehlerbilder	126
8.23 Praxislabor 3 – FSRM und Shadow Copies	107	10.14 Eventlogs und Fehlercodes	126
8.24 Praxislabor 4 – DFS Namespace	107	10.15 Systematisches Troubleshooting	126
8.25 Systematisches Troubleshooting	108	10.16 PowerShell und Diagnosebefehle	127
8.26 Fachgespräch – typische Fragen	108	10.17 Praxislabor 1 – Kerberos-Basis beobachten	127
8.27 Schnellreferenz	109	10.18 Praxislabor 2 – SPN untersuchen	127
8.28 Abschlusscheckliste	109		

10.19 Praxislabor 3 – Double-Hop	128	12.13 Shared-Nothing Live Migration	151
10.20 Praxislabor 4 – Clock-Skew-Fehler	128	12.14 Hyper-V Replica	151
10.21 Fachgespräch – typische Fragen	128	12.15 VM-Export, Import und Templates	152
10.22 Schnellreferenz	129	12.16 Integration Services und Gastzustand	152
10.23 Abschlusscheckliste	129	12.17 Hyper-V-Sicherheit	152
Kapitel 11 – PKI mit Active Directory Certificate Services	130	12.18 Vorbereitung auf Failover Clustering	152
11.1 Was ist eine PKI?	130	12.19 PowerShell-Schnellstart: VM erstellen	153
11.2 Symmetrisch, asymmetrisch und Hashing	131	12.20 Systematisches Hyper-V-Troubleshooting	153
11.3 Zertifikatsinhalt: Was steht wirklich darin?	131	12.21 Typische Fehlerbilder	154
11.4 CA-Typen in AD CS	132	12.22 Praxislabor 1 – SET-vSwitch und Host-vNICs	154
11.5 Unsere Lab-PKI	132	12.23 Praxislabor 2 – VM bereitstellen	154
11.6 ROOTCA01 – Offline Root CA installieren	133	12.24 Praxislabor 3 – Live Migration	154
11.7 AIA und CRL Distribution Points	133	12.25 Praxislabor 4 – Hyper-V Replica	155
11.8 PKI01 – Enterprise Issuing CA installieren	134	12.26 Fachgespräch – typische Fragen	155
11.9 Die Zertifikatskette verstehen	134	12.27 Schnellreferenz	156
11.10 Certificate Templates	135	12.28 Abschlusscheckliste	156
11.11 Enrollment und Autoenrollment	136	Kapitel 13 – Failover Clustering	157
11.12 Was passiert bei einer Zertifikatsanforderung?	136	13.1 Lernziele	157
11.13 Zertifikatsstores unter Windows	137	13.2 Was ist ein Failover Cluster?	157
11.14 Sperren, CRL und OCSP	137	13.3 Voraussetzungen und Cluster Validation	158
11.15 Online Responder / OCSP	138	13.4 Quorum – warum der Cluster abstimmen muss	158
11.16 LDAPS auf Domain Controllern	138	13.5 Quorum-Modelle und Witness	158
11.17 Schlüssellänge und Algorithmen	139	13.6 Witness richtig platzieren	159
11.18 CA-Backup und Recovery	139	13.7 Split Brain verstehen	159
11.19 PKI-Troubleshooting – systematische Reihenfolge	140	13.8 Cluster Networks und Heartbeat	159
11.20 Relevante Tools und Eventlogs	140	13.9 Cluster Shared Volumes (CSV)	160
11.21 Praxislabor 1 – Zweistufige PKI aufbauen	141	13.10 Shared Storage: iSCSI, FC und SMB	160
11.22 Praxislabor 2 – Zertifikatvorlage und Autoenrollment	141	13.11 Clusterrollen und Ressourcen	161
11.23 Praxislabor 3 – LDAPS auf DC01/DC02	141	13.12 Hochverfügbare Hyper-V-VMs	161
11.24 Praxislabor 4 – Zertifikat sperren und Revocation prüfen	142	13.13 Live Migration im Cluster	161
11.25 PKI-Sicherheitsregeln für Administratoren	142	13.14 Pause, Drain und Resume	161
11.26 Fachgespräch – typische Fragen	142	13.15 Failover, Failback und Preferred Owners	162
11.27 Schnellreferenz	143	13.16 Cluster Heartbeat und Schwellenwerte	162
11.28 Abschlusscheckliste	144	13.17 Cluster Validation im Detail	162
Kapitel 12 – Hyper-V	146	13.18 Typische Ausfallszenarien	163
12.1 Lernziele	146	13.19 Systematisches Cluster-Troubleshooting	163
12.2 Hyper-V-Architektur	146	13.20 Praxislabor 1 – Zwei-Node-Cluster aufbauen	163
12.3 Generation 1 vs. Generation 2	147	13.21 Praxislabor 2 – CSV bereitstellen	164
12.4 CPU und Arbeitsspeicher	147	13.22 Praxislabor 3 – Hochverfügbare VM	164
12.5 Virtuelle Switches	148	13.23 Praxislabor 4 – Fehler gezielt erzeugen	164
12.6 Switch Embedded Teaming (SET)	148	13.24 PowerShell-Schnellreferenz	165
12.7 Host-vNICs und VLANs	148	13.25 Fachgespräch – typische Fragen	165
12.8 VM-Netzwerkkarten und VLAN-Modi	149	13.26 Abschlusscheckliste	166
12.9 Virtuelle Festplatten und Storage	149	Kapitel 14 – PowerShell für Administratoren	168
12.10 Storage-Pfade und I/O	150	14.1 Lernziele	168
12.11 Checkpoints	150	14.2 Cmdlets und Verb-Noun-Konzept	168
12.12 Live Migration	150	14.3 Die Objektpipeline	169

14.4 Properties, Methods und Get-Member	169	15.2 Symptom, Ursache und Folgefehler	181
14.5 Variablen, Arrays und Hashtables	169	15.3 Der 8-Schritte-Prozess	182
14.6 Splatting	170	15.4 Scope zuerst	182
14.7 Filtern: möglichst früh und serverseitig	170	15.5 Zeitachse und letzte Änderungen	183
14.8 Select, Sort, Group und Measure	170	15.6 Baseline und Vergleichssystem	183
14.9 Calculated Properties	170	15.7 Layer-Modell für die Diagnose	183
14.10 Import und Export	171	15.8 Hypothesen statt Befehlsroulette	184
14.11 foreach, ForEach-Object und Schleifen	171	15.9 Beweise sichern, bevor man ändert	184
14.12 Bedingungen und switch	171	15.10 Windows Event Logs gezielt nutzen	184
14.13 Funktionen für Administratoren	172	15.11 Netzwerk-Basisdiagnose	185
14.14 Advanced Functions und Parameter	172	15.12 DNS-Troubleshooting	185
14.15 Fehlerbehandlung	172	15.13 Active-Directory-Diagnose	186
14.16 \$Error, ErrorRecord und Throw	173	15.14 Kerberos und Zeit	186
14.17 Logging und Transcripts	173	15.15 GPO-Troubleshooting	186
14.18 PowerShell Remoting	173	15.16 Fileserver und Berechtigungen	187
14.19 Der Double-Hop bei Remoting	174	15.17 Hyper-V-Troubleshooting	187
14.20 CIM statt alter WMI-Technik	174	15.18 Failover-Cluster-Troubleshooting	188
14.21 Credentials und sensible Daten	174	15.19 Performance-Troubleshooting	188
14.22 Execution Policy und Skriptsignierung	175	15.20 Tracing und Paketmitschnitt	188
14.23 Module	175	15.21 Änderungen: klein, reversibel, dokumentiert	189
14.24 PowerShell Profiles	175	15.22 Verifikation und Abschluss	189
14.25 ShouldProcess, -WhatIf und -Confirm	176	15.23 Diagnoseprotokoll – Minimalstandard	189
14.26 Administrative Beispiele	176	15.24 Praxislabor 1 – Client findet keinen DC	190
14.27 Praxislabor 1 – Pipeline und Objekte	177	15.25 Praxislabor 2 – GPO wirkt nicht	190
14.28 Praxislabor 2 – Server-Health-Check	177	15.26 Praxislabor 3 – Fileserver „Berechtigungsproblem“	190
14.29 Praxislabor 3 – Remoting	177	15.27 Praxislabor 4 – Clusterrolle fällt aus	191
14.30 Praxislabor 4 – Robustes Administrationsskript	178	15.28 Praxislabor 5 – Unbekannter Fehler als Teamübung	191
14.31 Typische Fehlerbilder	178	15.29 Typische Anti-Patterns	191
14.32 Fachgespräch – typische Fragen	178	15.30 Fachgespräch – typische Fragen	191
14.33 Schnellreferenz	179	15.31 Schnellreferenz	192
14.34 Abschlusscheckliste	179	15.32 Abschlusscheckliste	192
Kapitel 15 – Troubleshooting-Methodik	181		
15.1 Lernziele	181		

Vorwort und Arbeitsweise

Dieses Handbuch führt dich durch die Kernthemen der Windows-Server-Administration: von der Architektur von Active Directory über DNS, DHCP und Routing bis zu Gruppenrichtlinien, Fileserver, Security, Kerberos, PKI, Hyper-V und Failover-Clustering. Zwei Kapitel am Ende vermitteln die Werkzeuge, mit denen Administratoren dauerhaft arbeiten: PowerShell und eine feste Methodik für die Fehlersuche.

Der rote Faden ist Verständnis statt Klick-Anleitung. Jeder Konfigurationsschritt wird mit der Funktion dahinter verbunden. Wer weiß, *warum* ein DC über SRV-Records gefunden wird oder warum Kerberos auf die Uhrzeit achtet, kann Fehler eingrenzen, statt Dienste auf Verdacht neu zu starten.

Für wen ist das Buch?

Für angehende und praktizierende Systemadministratoren, die Windows-Server-Umgebungen aufbauen, betreiben und absichern: IT-Umsteiger, Teilnehmer von Administrator-Ausbildungen, Helpdesk-Mitarbeiter auf dem Weg in die Server-Administration und erfahrene Admins, die Wissenslücken schließen oder nachschlagen wollen. Grundkenntnisse in Windows und Netzwerken sind hilfreich, aber keine Voraussetzung für die ersten Kapitel.

So ist jedes Kapitel aufgebaut

Lernziele	Was du nach dem Kapitel erklären und tun kannst.
Konzept	Wie die Technik funktioniert, mit Tabellen und Merkkästen.
Schritt für Schritt	Konfiguration mit GUI und PowerShell, jeweils mit Kontrolle des Ergebnisses.
Troubleshooting	Typische Fehlerbilder und ein reproduzierbarer Ablauf zur Eingrenzung.
Praxislabore	Aufgaben im Lab, teils mit bewusst eingebauten Fehlern.
Fachgespräch	Typische Fragen mit kurzen Antworten, ideal zur Vorbereitung auf Prüfung und Vorstellungsgespräch.
Abschlusscheckliste	Kontrolle, ob die Lernziele erreicht sind.
Schnellreferenz	Die wichtigsten Befehle auf einen Blick zum Nachschlagen.

Nicht jedes Kapitel enthält alle Bausteine; die Gewichtung folgt dem Thema.

Empfohlener Lernpfad

Die Kapitel bauen aufeinander auf. Wer von vorne durcharbeitet, kann alle Labs in derselben Umgebung nachvollziehen. Zum Nachschlagen genügen die Schnellreferenzen und das ausführliche Inhaltsverzeichnis.

Kapitel	Block	Inhalt
1-4	AD-Fundament	Architektur, Replikation, FSMO und DNS bilden das Fundament. Fast jeder spätere Fehler hängt hier zusammen.
5-6	Netzwerk-Dienste	DHCP, IP-Adressierung und Routing, damit Clients Server überhaupt erreichen.
7-8	Verwalten	Gruppenrichtlinien, Fileserver und Berechtigungen im Alltag.
9-11	Absichern	Security-Baseline, Kerberos und eine eigene PKI.
12-13	Plattform	Hyper-V und Failover Clustering als Basis für hochverfügbare Dienste.
14-15	Profi-Werkzeuge	PowerShell-Automatisierung und eine feste Methodik für die Fehlersuche.

Arbeite mit einem Lab

Die Praxislabore sind für eine isolierte Testumgebung gedacht, zum Beispiel auf Hyper-V mit eigenem virtuellen Switch. Dort kannst du Fehler gezielt erzeugen und wieder beheben, ohne ein Produktivsystem zu gefährden. Lege vor größeren Änderungen einen Checkpoint an.

Die Lab-Umgebung

Alle Beispiele des Buches nutzen dieselbe fiktive Schulungsumgebung. Die Domäne `kurs.at` ist ein reiner Lab-Name; in produktiven Umgebungen sollte der interne Namensraum bewusst geplant und eindeutig verwaltet werden. Welche Systeme ein Kapitel benötigt, steht jeweils am Kapitelanfang und in den Lab-Abschnitten.

System	Rolle
kurs.at	Lab-Domäne (Gesamtstruktur) für alle Kapitel
192.168.1.0/24 und 192.168.2.0/24	Die beiden Lab-Netze (Standort 1 und Standort 2)
DC01 (192.168.1.10) · DC02 (192.168.2.11)	Domain Controller mit DNS und Global Catalog
RTR01 (192.168.1.254 / 192.168.2.254)	Windows-Router zwischen den beiden Netzen
FS01 (192.168.1.20)	Fileserver (Kapitel 8)
DHCP01 (192.168.1.30) · DHCP02 (192.168.2.30)	DHCP-Server mit Failover (Kapitel 5)
CLIENT01	Windows-Client für Tests
ROOTCA01 · PKI01	Offline Root CA und Enterprise Issuing CA (Kapitel 11)
HV01 · HV02	Hyper-V-Hosts und Cluster-Nodes (Kapitel 12 und 13)
APP01	Beispiel-VM für Live Migration und Replica

Die Adressen sind Beispielwerte und können im eigenen Lab abweichen. Wichtig ist, dass beide Netze über RTR01 verbunden sind und die Namensauflösung über die Domain Controller läuft.

KAPITEL 15

Troubleshooting-Methodik

Strukturiert diagnostizieren, Ursachen eingrenzen, Änderungen verifizieren

15.1 Lernziele

- Fehler systematisch statt durch Versuch und Irrtum eingrenzen.
- Symptome, Ursachen und Folgefehler klar voneinander unterscheiden.
- Abhängigkeiten zwischen Netzwerk, DNS, AD, Kerberos, GPO und Diensten erkennen.
- Baseline, Zeitachse, Scope und letzte Änderungen als Diagnosewerkzeuge nutzen.
- Windows-Werkzeuge und PowerShell gezielt für Evidenzgewinn einsetzen.
- Änderungen kontrolliert durchführen und anschließend technisch verifizieren.
- Diagnoseergebnisse so dokumentieren, dass andere Administratoren sie nachvollziehen können.

Kernidee:

Gutes Troubleshooting ist kein Sammeln möglichst vieler Befehle. Es ist ein reproduzierbarer Prozess: Problem definieren, Scope bestimmen, Hypothese bilden, Evidenz sammeln, Änderung durchführen und Ergebnis verifizieren.

15.2 Symptom, Ursache und Folgefehler

Ein sichtbarer Fehler ist häufig nur das letzte Glied einer Kette. Wer das Symptom mit der Ursache verwechselt, repariert oft an der falschen Stelle.

Beobachtung	Mögliche Ursache	Typischer Folgefehler
Domänenanmeldung langsam	DNS-Auflösung oder DC-Locator fehlerhaft	GPO-Verarbeitung verzögert
Netzlaufwerk fehlt	GPO nicht angewendet	Benutzer meldet Fileserver-Problem
Live Migration scheitert	Kerberos/Delegation oder Netzwerkproblem	VM bleibt auf Quellhost
LDAPS funktioniert nicht	Zertifikat/EKU/SAN/Kette fehlerhaft	Anwendung meldet LDAP-Verbindungsfehler
Clusterrolle offline	Storage- oder Netzwerkabhängigkeit gestört	Dienst ist aus Clientsicht nicht verfügbar

Diagnosedisziplin:

Die erste Frage lautet nicht „Welcher Dienst ist kaputt?“, sondern „Was ist sicher beobachtet und was ist nur eine Vermutung?“

15.3 Der 8-Schritte-Prozess

Schritt	Frage	Ergebnis
1. Problem definieren	Was genau funktioniert nicht?	Reproduzierbares Symptom
2. Scope bestimmen	Wer/was ist betroffen?	Ein Client, Site, Server, Domäne, Cluster?
3. Zeitachse	Seit wann? Was änderte sich?	Startpunkt und Change-Korrelation
4. Baseline	Was wäre normal?	Vergleichswert
5. Hypothese	Welche Schicht/Abhängigkeit passt zum Symptom?	Priorisierte Ursache
6. Evidenz	Welche Messung bestätigt oder widerlegt die Hypothese?	Logs, Tests, Statusdaten
7. Änderung	Was ist die kleinste sinnvolle Korrektur?	Kontrollierter Fix
8. Verifikation	Ist das Problem wirklich behoben?	Funktionstest + Folgewirkungen prüfen

15.4 Scope zuerst

Der Scope reduziert die Anzahl möglicher Ursachen drastisch. Ein Problem auf einem Client verlangt eine andere Strategie als derselbe Fehler auf allen Clients einer Site.

Scope	Wahrscheinliche Richtung
Nur ein Benutzer	Profil, Gruppenmitgliedschaft, Token, persönliche Einstellungen
Nur ein Client	lokale Konfiguration, Cache, Netzwerkadapter, lokale Firewall
Alle Clients eines VLANs	DHCP, Routing, ACL, DNS-Optionen, Gateway
Alle Clients einer Site	Site-Link, WAN, lokaler DC/DNS, Routing
Alle Domänenbenutzer	AD/DNS/Kerberos, zentrale GPO, DC-Erreichbarkeit
Nur ein Cluster-Node	Host-Netz, Storagepfad, Treiber, Node-Status

15.5 Zeitachse und letzte Änderungen

- Wann trat das Problem erstmals auf?
- War es davor sicher funktionsfähig?
- Gab es Patchen, Reboots, GPO-Änderungen, Zertifikatswechsel, Netzwerkänderungen oder Storage-Arbeiten?
- Trat der Fehler unmittelbar nach einer Änderung auf oder erst später?
- Wurde ein automatisierter Prozess aktiv, z. B. Zertifikats-Renewal, DHCP-Lease, GPO-Refresh oder Backup?

Wichtig:

„Es wurde nichts geändert“ ist keine belastbare Aussage. Prüfe Change-Tickets, Eventlogs, Gruppenrichtlinien, geplante Tasks, Patch-Zeitpunkte und Konfigurationshistorie.

15.6 Baseline und Vergleichssystem

Ein gesundes Vergleichssystem ist oft wertvoller als zehn zufällige Internet-Suchtreffer. Vergleiche möglichst gleiche Rollen, Sites und Softwarestände.

```
Get-ComputerInfo | Select WindowsProductName,WindowsVersion,OsBuildNumber
Get-NetIPConfiguration
Get-DnsClientServerAddress
w32tm /query /status
```

15.7 Layer-Modell für die Diagnose

Das OSI-Modell ist als Denkmodell nützlich. In Windows-Umgebungen arbeitet man praktisch häufig von unten nach oben: Link, IP, Name Resolution, Transport, Authentifizierung, Anwendung.

Ebene	Prüffrage	Beispiele
Link	Ist das Interface aktiv?	NIC, VLAN, vSwitch, Switchport
IP	Stimmen Adresse, Maske, Gateway und Route?	ipconfig, Get-NetIPConfiguration, route print
Name Resolution	Wird der richtige Name zur richtigen IP aufgelöst?	Resolve-DnsName, nslookup
Transport	Ist der notwendige Port erreichbar?	Test-NetConnection
Authentifizierung	Kerberos/NTLM/Ticket/Zeitsync korrekt?	klist, nltest, w32tm
Anwendung	Läuft der Dienst und verarbeitet er Anfragen?	Services, Eventlogs, eigene Logs

15.8 Hypothesen statt Befehlsroulette

Jeder Test sollte eine konkrete Frage beantworten. Ein Test ohne erwartetes Ergebnis liefert Daten, aber kaum Erkenntnis.

Hypothese	Test	Interpretation
DNS zeigt auf falschen Server	Resolve-DnsName DC01.kurs.at	Falsche IP bestätigt DNS-Richtung
SMB-Port blockiert	Test-NetConnection FS01 -Port 445	TCP-Test trennt Netzwerk/Firewall von SMB-Anwendung
Kerberos-Ticket fehlt	klist	Kein passendes Service Ticket -> SPN/Name/Authentifizierung prüfen
AD-Replikation gestört	repadmin /replsummary	Fehlerpartner und Richtung sichtbar
Cluster-Netz gestört	Get-ClusterNetwork	Status und Rollen der Cluster-Netze vergleichen

15.9 Beweise sichern, bevor man ändert

- Fehlermeldung inklusive Zeitstempel und Event-ID erfassen.
- Konfiguration vor der Änderung dokumentieren.
- Bei wiederkehrenden Fehlern Logs exportieren, bevor sie überschrieben werden.
- Bei Netzwerkproblemen Paketmitschnitt oder Trace vor dem Fix erwägen.
- Bei Cluster-/Storage-Problemen Clusterlog und Storagezustand sichern.

```
wevtutil epl System C:\Temp\System.evtx
wevtutil epl "Directory Service" C:\Temp\DirectoryService.evtx
Get-ClusterLog -UseLocalTime -Destination C:\Temp\ClusterLogs
```

15.10 Windows Event Logs gezielt nutzen

Nicht jedes rote Event ist die Ursache. Entscheidend sind Zeitpunkt, Quelle, Korrelation und Wiederholbarkeit.

Bereich	Wichtige Logs
AD DS	Directory Service, DFS Replication, DNS Server, System
GPO	Microsoft-Windows-GroupPolicy/Operational
Kerberos/Security	Security, System, Kerberos-bezogene Ereignisse
Hyper-V	Hyper-V-VMMS/Admin, Hyper-V-Worker/Admin
Failover Cluster	Microsoft-Windows-FailoverClustering/Operational, System
PowerShell	Microsoft-Windows-PowerShell/Operational

```
Get-WinEvent -FilterHashtable @{LogName="System"; Level=2; StartTime=(Get-Date).AddHours(-2)} |  
Select TimeCreated,ProviderName,Id,Message
```

15.11 Netzwerk-Basisdiagnose

Schritt 1: Interface und IP-Konfiguration prüfen.

Schritt 2: Lokales Gateway testen.

Schritt 3: Ziel-IP direkt testen.

Schritt 4: DNS-Auflösung getrennt prüfen.

Schritt 5: Erforderliche TCP/UDP-Dienste gezielt testen.

Schritt 6: Route und gegebenenfalls MTU prüfen.

```
Get-NetAdapter  
Get-NetIPConfiguration  
ping 192.168.1.254  
tracert DC01.kurs.at  
Test-NetConnection DC01.kurs.at -Port 389  
route print
```

Merksatz:

Ping ist kein allgemeiner Verfügbarkeitstest. ICMP kann blockiert sein, während der eigentliche Dienst funktioniert. Teste den Dienstport.

15.12 DNS-Troubleshooting

Schritt 1: Welchen DNS-Server verwendet der Client?

Schritt 2: Kann der Client den DNS-Server erreichen?

Schritt 3: Forward- und Reverse-Auflösung testen.

Schritt 4: AD-SRV-Records prüfen.

Schritt 5: Cache und alte Records berücksichtigen.

Schritt 6: Bei AD-Problemen DNS-Replikation und Zonenstatus prüfen.

```
Get-DnsClientServerAddress  
Resolve-DnsName DC01.kurs.at  
Resolve-DnsName _ldap._tcp.dc._msdcs.kurs.at -Type SRV  
ipconfig /displaydns  
ipconfig /flushdns  
dcdiag /test:dns /e /v
```

15.13 Active-Directory-Diagnose

```
repadmin /replsummary
repadmin /showrepl DC01
dcdiag /e /v
nltest /dsgetdc:kurs.at
nltest /dsgetsite
```

Symptom	Erste Richtung
Benutzer kann sich nicht anmelden	DNS, DC-Locator, Zeit, Kerberos, Konto
Objekt nur auf einem DC sichtbar	Replikation und Partition prüfen
SYSVOL fehlt	DFSR/SYSVOL separat von AD-Objektreplication prüfen
Client nutzt entfernten DC	Sites/Subnets und DC-Locator prüfen

15.14 Kerberos und Zeit

```
klist
klist purge
w32tm /query /status
w32tm /query /source
setspn -Q HTTP/app01.kurs.at
```

Praxis:

Kerberos-Fehler wirken häufig wie Anwendungs- oder Berechtigungsprobleme. Vor tiefem Applikationsdebugging immer Name, SPN, Zeit und Ticket prüfen.

15.15 GPO-Troubleshooting

Schritt 1: Liegt Benutzer/Computer in der erwarteten OU?

Schritt 2: Ist die GPO korrekt verlinkt und aktiviert?

Schritt 3: Greifen Security Filtering oder WMI Filter?

Schritt 4: Block Inheritance / Enforced / Link Order prüfen.

Schritt 5: gpresult und GroupPolicy Operational Log auswerten.

Schritt 6: Bei SYSVOL-Problemen DFSR und DC-Erreichbarkeit prüfen.

```
gpupdate /force
gpresult /h C:\Temp\gp.html
gpresult /r
Get-GPResultantSetOfPolicy -ReportType Html -Path C:\Temp\rsop.html
```

15.16 Fileserver und Berechtigungen

Bei Fileserver-Problemen müssen Share-Rechte, NTFS-Rechte, Gruppenmitgliedschaften, Token und Erreichbarkeit getrennt betrachtet werden.

```
Test-NetConnection FS01 -Port 445
whoami /groups
icacls D:\Daten
Get-SmbShare
Get-SmbSession
```

Frage	Werkzeug
Ist SMB erreichbar?	Test-NetConnection -Port 445
Welche Gruppen enthält der Token?	whoami /groups
Welche ACL liegt auf dem Ordner?	icacls / Get-Acl
Ist der Share vorhanden?	Get-SmbShare
Gibt es aktive Sessions/Dateien?	Get-SmbSession / Get-SmbOpenFile

15.17 Hyper-V-Troubleshooting

```
Get-VM
Get-VMSwitch
Get-VMNetworkAdapter -All
Get-VHD -Path D:\VMs\VM01\disk.vhdx
Get-VMHost
```

- VM-Status und VMMS/Worker-Events prüfen.
- vSwitch/VLAN und physische NIC getrennt prüfen.
- VHDX-Pfad, Berechtigungen und freien Speicher kontrollieren.
- Bei Migration: Netzwerk, Authentifizierung und Kompatibilität prüfen.
- Bei Storageproblemen niemals nur die VM-Konsole betrachten.

15.18 Failover-Cluster-Troubleshooting

```
Get-ClusterNode
Get-ClusterGroup
Get-ClusterResource
Get-ClusterNetwork
Get-ClusterSharedVolume
Get-ClusterLog -UseLocalTime -TimeSpan 15
```

Schritt 1: Ist der Cluster selbst online und haben die Nodes Quorum?

Schritt 2: Welche Rolle/Ressource ist tatsächlich fehlerhaft?

Schritt 3: Welche Abhängigkeit dieser Ressource ist offline?

Schritt 4: Sind Cluster Networks und CSVs gesund?

Schritt 5: Clusterlog und Eventlog zeitlich korrelieren.

Schritt 6: Erst danach Failover/Restart oder Konfigurationsänderungen durchführen.

15.19 Performance-Troubleshooting

Hohe CPU, RAM- oder I/O-Auslastung ist zunächst eine Beobachtung. Entscheidend ist, welcher Prozess oder Workload die Ressource konsumiert und ob dies gegenüber der Baseline ungewöhnlich ist.

```
Get-Process | Sort CPU -Descending | Select -First 10 Name,Id,CPU,WorkingSet
Get-Counter "\Processor(_Total)\% Processor Time"
Get-Counter "\Memory\Available MBytes"
```

Ressource	Frage	Werkzeuge
CPU	Welcher Prozess? dauerhaft oder Peak?	Task Manager, Get-Process, PerfMon
RAM	Commit/Working Set/Paging?	Task Manager, Resource Monitor, PerfMon
Disk	Latenz, Queue, Durchsatz?	PerfMon, Resource Monitor, Storage-Tools
Netz	Fehler, Drops, Bandbreite?	Get-NetAdapterStatistics, PerfMon, Switch/NIC

15.20 Tracing und Paketmitschnitt

Wenn Statusabfragen nicht reichen, kann ein Trace zeigen, ob Pakete gesendet, beantwortet, abgelehnt oder gar nicht erst übertragen werden.

```
pktmon start --capture --comp nics --pkt-size 0
# Problem reproduzieren
pktmon stop
pktmon etl2pcap PktMon.etl --out C:\Temp\trace.pcapng
```

Praxis:

Ein Paketmitschnitt ersetzt keine Hypothese. Vorher festlegen, welche Verbindung, IPs, Ports und Zeitspanne untersucht werden.

15.21 Änderungen: klein, reversibel, dokumentiert

- Nur eine wesentliche Variable gleichzeitig ändern.
- Vorher Soll- und Ist-Zustand sichern.
- Rollback definieren.
- Keine „vorsorglichen“ Änderungen an mehreren Systemen gleichzeitig.
- Nach Änderung exakt denselben Test wie vorher wiederholen.
- Folgewirkungen kontrollieren.

Anti-Pattern:

Wenn fünf Dinge gleichzeitig geändert werden und es danach funktioniert, weiß niemand, was die Ursache war – und niemand weiß, welche Änderung später Nebenwirkungen erzeugt.

15.22 Verifikation und Abschluss

Schritt 1: Ursprüngliches Symptom erneut testen.

Schritt 2: Gesunden Sollzustand mit Messwerten bestätigen.

Schritt 3: Relevante Logs auf neue Fehler prüfen.

Schritt 4: Bei redundanten Systemen auch Partner/Failoverpfad testen.

Schritt 5: Dokumentieren: Ursache, Fix, Verifikation und Prävention.

15.23 Diagnoseprotokoll – Minimalstandard

Feld	Beispiel
Zeit	10:32 - Benutzer meldet Anmeldeproblem
Scope	Alle Clients VLAN 20, VLAN 10 nicht betroffen
Symptom	DC Locator schlägt fehl

Feld	Beispiel
Evidenz	DNS-Option zeigt auf alten DNS-Server
Ursache	DHCP Option 006 nach Migration nicht angepasst
Änderung	DNS-Option korrigiert, Lease erneuert
Verifikation	nltest /dsgetdc und Anmeldung erfolgreich
Prävention	DHCP-Konfigurationscheck in Change-Checkliste

15.24 Praxislabor 1 – Client findet keinen DC

Schritt 1: Auf CLIENT01 absichtlich einen falschen DNS-Server eintragen.

Schritt 2: Anmeldung/DC-Locator bzw. nltest testen und Fehler dokumentieren.

Schritt 3: IP, DNS und SRV-Auflösung systematisch prüfen.

Schritt 4: Ursache korrigieren.

Schritt 5: Denselben Test erneut durchführen und Ergebnis dokumentieren.

```
ipconfig /all
Resolve-DnsName _ldap._tcp.dc._msdcs.kurs.at -Type SRV
nltest /dsgetdc:kurs.at
```

15.25 Praxislabor 2 – GPO wirkt nicht

Schritt 1: Eine Test-GPO an die falsche OU verlinken oder Security Filtering falsch setzen.

Schritt 2: Auf CLIENT01 gpupdate ausführen und erwartete Einstellung prüfen.

Schritt 3: gpresult-Bericht erzeugen.

Schritt 4: Ursache aus Scope, Link und Filtering ableiten.

Schritt 5: Korrektur durchführen und erneut verifizieren.

15.26 Praxislabor 3 – Fileserver „Berechtigungsproblem“

Schritt 1: Benutzer bewusst aus einer benötigten Berechtigungsgruppe entfernen.

Schritt 2: Zugriff auf \\FS01\\Daten testen.

Schritt 3: Port 445, Share, Token und NTFS-ACL getrennt prüfen.

Schritt 4: Gruppenmitgliedschaft korrigieren und neuen Logontoken erzeugen.

Schritt 5: Zugriff erneut testen.

15.27 Praxislabor 4 – Clusterrolle fällt aus

Schritt 1: Eine ungefährliche Lab-Ressource kontrolliert offline nehmen oder einen Node pausieren.

Schritt 2: Clusterrolle, Ressource, Abhängigkeiten und Owner Node prüfen.

Schritt 3: Clusterlog für den Zeitraum erzeugen.

Schritt 4: Ursache und erwartetes Clusterverhalten beschreiben.

Schritt 5: Ressource kontrolliert wiederherstellen und Clusterzustand verifizieren.

15.28 Praxislabor 5 – Unbekannter Fehler als Teamübung

Der Trainer präpariert einen Fehler, ohne die Ursache zu nennen. Die Teilnehmer dürfen keine Konfiguration ändern, bevor sie Problemdefinition, Scope, Hypothese und mindestens zwei Evidenzpunkte dokumentiert haben.

Didaktisches Ziel:

Dieses Labor prüft Methodik statt Gedächtnis. Bewertet wird nicht, wer am schnellsten klickt, sondern wer den Fehler reproduzierbar eingrenzt und den Fix sauber verifiziert.

15.29 Typische Anti-Patterns

Anti-Pattern	Warum problematisch
Blind Dienste neu starten	Symptom verschwindet, Ursache bleibt unbekannt
Mehrere Änderungen gleichzeitig	Keine Zuordnung zwischen Fix und Wirkung möglich
Nur Event Viewer öffnen	Logs ohne Hypothese erzeugen viel Rauschen
Ping = funktioniert	ICMP sagt nichts über LDAP, SMB, HTTPS oder Kerberos aus
Cache sofort löschen	Wichtige Evidenz kann verloren gehen
„Server ist schuld“	Keine technische Eingrenzung
Nur GUI verwenden	Schwer reproduzierbar und schlecht dokumentierbar

15.30 Fachgespräch – typische Fragen

Frage	Musterantwort
Was ist der erste Schritt beim Troubleshooting?	Das Problem präzise und reproduzierbar definieren.
Warum ist Scope wichtig?	Er grenzt die Menge möglicher Ursachen stark ein.
Was ist eine Baseline?	Ein bekannter gesunder Vergleichszustand.

Frage	Musterantwort
Warum nur eine Variable ändern?	Damit Wirkung und Ursache eindeutig zugeordnet werden können.
Warum ist Ping allein ungeeignet?	Weil ICMP-Erreichbarkeit nicht die Verfügbarkeit eines konkreten Dienstes beweist.
Wann ist ein Incident abgeschlossen?	Wenn Funktion wiederhergestellt, Ergebnis verifiziert und Ursache/Fix dokumentiert sind.

15.31 Schnellreferenz

Bereich	Werkzeuge
Netzwerk	Get-NetIPConfiguration, ping, tracert, route print, Test-Net-Connection
DNS	Resolve-DnsName, nslookup, dcdiag /test:dns
AD	repadmin, dcdiag, nltest
Kerberos/Zeit	klist, setspn, w32tm
GPO	gpupdate, gpresult, GroupPolicy Operational Log
Fileserver	icacls, Get-Acl, Get-SmbShare, Get-SmbSession
Hyper-V	Get-VM, Get-VMSwitch, Get-VMNetworkAdapter, Get-VHD
Cluster	Get-ClusterNode, Get-ClusterGroup, Get-ClusterLog
Events	Get-WinEvent, wevtutil
Trace	pktmon

15.32 Abschlusscheckliste

- Ist das Symptom reproduzierbar und präzise beschrieben?
- Ist klar, wer oder was betroffen ist?
- Ist die Zeitachse bekannt?
- Gibt es einen gesunden Vergleichswert?
- Wurde eine Hypothese vor dem Test formuliert?
- Wurde Evidenz vor Änderungen gesichert?
- Wurde nur die notwendige Änderung durchgeführt?
- Wurde mit demselben Test verifiziert?
- Wurden Ursache, Fix und Prävention dokumentiert?

Abschluss:

Ein guter Systemadministrator löst nicht nur den aktuellen Fehler. Er hinterlässt eine nachvollziehbare Diagnose, einen kontrollierten Fix und idealerweise eine Maßnahme, die denselben Fehler künftig schneller erkennbar oder vermeidbar macht.

Das war die Leseprobe

Du hast das Inhaltsverzeichnis, das Vorwort, die Lab-Umgebung und das vollständige Kapitel 15 „Troubleshooting-Methodik“ gelesen. Das ganze Praxishandbuch umfasst:

- **194 Seiten** in 15 Kapiteln, von Active Directory über DNS, DHCP, Routing, Gruppenrichtlinien, Fileserver und Security bis zu Kerberos, PKI, Hyper-V, Failover-Clustering und PowerShell
- **Praxislabore** mit Schritt-für-Schritt-Ablauf und bewusst eingebauten Fehlern in jedem Kapitel
- **Fachgespräch-Fragen**, Abschlusschecklisten und Schnellreferenzen zum Nachschlagen
- Eine durchgehende Lab-Umgebung, sodass alle Beispiele aufeinander aufbauen

Passend dazu gibt es ein Zusatzpaket mit Multiple-Choice-Prüfungsfragen samt Lösungen.

Die Seitenzahlen im Inhaltsverzeichnis beziehen sich auf das vollständige Buch.