Inhaltsangabe / Übersicht

IT-Praxiswissen – verbindliche Inhaltsübersicht

Status: alleinige Referenz für die weitere Ausarbeitung

Diese Inhaltsübersicht ersetzt alle früheren Übersichten, provisorischen Nummerierungen und frei fortgesetzten Seitenfolgen.

Verbindliche Regeln:

- Jede BookStack-Seite erhält genau die hier angegebene Nummer und exakt den hier angegebenen Titel.
- Eine Nummer darf nicht frei ergänzt, verschoben oder doppelt vergeben werden.
- Neue Seiten werden zuerst in diese Inhaltsübersicht aufgenommen und erst danach ausgearbeitet.
- Unterpunkte innerhalb einer Seite dürfen als `x.y.1`, `x.y.2` und so weiter nummeriert werden. Sie sind keine eigenständigen BookStack-Seiten.
- Frühere Entwürfe bleiben nur verwendbar, wenn sie einem Titel dieser Übersicht eindeutig zugeordnet und vollständig neu nummeriert wurden.
- Die frühere Seite **„3.6 Erstdiagnose, Lösung und funktionale Eskalation“** wird verbindlich zu **1.6 Erstdiagnose, Lösung und funktionale Eskalation**.
- Die frühere Seite **„8.5 macOS – Prozesse, Dienste, Logs und Ressourcen diagnostizieren“** wird verbindlich zu **14.1 macOS – Prozesse, Dienste, Logs und Ressourcen diagnostizieren**. Auch alle internen Unterpunkte müssen von `8.5.x` auf `14.1.x` geändert werden.
- Kapitel 8 besitzt ausschließlich die Seiten 8.1 bis 8.4. Eine Seite 8.5 existiert nicht. Nach 8.4 folgt 9.1.

Kapitel 1 – Methodik, Dokumentation und Eskalation

- **1.1 Zweck, Aufbau und Grundregeln der Fehleranalyse**
- **1.2 Störung aufnehmen und Benutzer gezielt befragen**
- **1.3 Umfang, Auswirkung, Dringlichkeit und Priorität bestimmen**
- **1.4 Timeline, letzte Änderungen und Beweise sichern**
- **1.5 Hypothesen bilden und Diagnosemethoden auswählen**

Kapitel 2 – Grundwerkzeuge und Diagnosebefehle

Kapitel 3 – Strom, Hardware und physische Verbindung

Kapitel 4 – Ethernet, Switching und VLAN

Kapitel 5 – IPv4, IPv6, ARP, NDP und Routing

- **5.13 Systematischer Diagnoseablauf für IP und Routing**

Kapitel 6 – DHCP

- **6.1 DHCP-Grundlagen und DORA-Ablauf**
- **6.2 DHCP-Clientdienst und DHCP-Serverdienst**
- **6.3 Scope, Adresspool, Ausschlussbereich und Erschöpfung**
- **6.4 Reservierungen, Adresskonflikte und BAD_ADDRESS**
- **6.5 DHCP Relay, IP Helper, GIADDR und VLAN-Zuordnung**
- **6.6 UDP 67/68, Firewall und DHCP Snooping**
- **6.7 DHCP-Optionen für Gateway, DNS, Suffix, PXE und VoIP**
- **6.8 Rogue DHCP Server erkennen und eingrenzen**
- **6.9 AD-Autorisierung und Bindung an Netzwerkschnittstellen**
- **6.10 DHCP-Failover, Lease-Datenbank, Logs und alte Leases**
- **6.11 Systematischer DHCP-Diagnoseablauf mit Paketmitschnitt**

Kapitel 7 – DNS und Namensauflösung

- **7.1 DNS-Grundlagen und vollständiger Auflösungspfad**
- **7.2 Client-DNS, DNS-Server, Suffix, Kurzname und FQDN**
- **7.3 A-, AAAA-, CNAME-, PTR- und SRV-Records**
- **7.4 Zonen, Delegationen, Secondary Zones und Zonentransfers**
- **7.5 Dynamische Updates und AD-integrierte Replikation**
- **7.6 Forwarder und Conditional Forwarder**
- **7.7 DNS-Cache, negative Antworten, hosts-Datei und Suchdomänen**
- **7.8 Split-DNS, VPN-DNS, öffentliche Resolver, DoH und DoT**
- **7.9 IPv6- und AAAA-Bevorzugung bei fehlerhaftem IPv6-Pfad**
- **7.10 DNSSEC, EDNS, MTU sowie UDP und TCP 53**
- **7.11 DNS-Leistung und fehlerhafte Reverse-Lookups**
- **7.12 Systematischer DNS-Diagnoseablauf**

Kapitel 8 – Zeit, NTP und Zeitzonen

- **8.1 Systemzeit, UTC, Zeitzone und Zeitabweichung**
- **8.2 NTP-Quellen, Erreichbarkeit, Synchronisationsstatus und Drift**
- **8.3 Windows-Domänenzeit und Kerberos-Zeitfehler**

- **8.4 Zeitfehler bei Linux, macOS, virtuellen Maschinen, Zertifikaten, Tokens und Logs**

Kapitel 9 – TCP, UDP, Ports, Firewall, NAT und Proxy

- **9.1 Ports, Sockets, Listener und gebundene Adressen**
- **9.2 TCP-Handshake, Timeouts und TCP Reset**
- **9.3 UDP-Diagnose und ICMP-Fehlermeldungen**
- **9.4 Lokale Host-Firewall prüfen**
- **9.5 Netzwerkfirewall, ACL-Reihenfolge und Stateful Inspection**
- **9.6 Asymmetrische Pfade, Sessiontabellen und Connection Tracking**
- **9.7 Ephemeral Ports und Verbindungsgrenzen**
- **9.8 NAT, Portweiterleitung und Hairpin NAT im Datenpfad**
- **9.9 Proxy, PAC-Datei und Proxy-Authentifizierung**
- **9.10 TLS-Inspection und Zertifikatsfehler**
- **9.11 Load Balancer, Healthchecks, Backends und Session Persistence**
- **9.12 Reverse Proxy, Header, WAF und Rate Limits**
- **9.13 Retransmissions, Zero Window und MTU-Probleme**
- **9.14 Systematischer Diagnoseablauf: Ping funktioniert, Anwendung nicht**

Kapitel 10 – WLAN

- **10.1 WLAN-Grundlagen, Frequenzbänder und Sicherheitsverfahren**
- **10.2 WLAN deaktiviert, falsche SSID oder falscher Schlüssel**
- **10.3 WPA2-, WPA3- und Client-Inkompatibilitäten**
- **10.4 802.1X, EAP, RADIUS und Zertifikate**
- **10.5 Association, Authentifizierung und anschließender DHCP-Ablauf**
- **10.6 Signalstärke, SNR, Reichweite und Dämpfung**
- **10.7 Interferenz, Kanalauslastung, Kanalplanung und Kanalbreite**
- **10.8 Regulatory Domain, DFS und Radarwechsel**
- **10.9 Roaming, Sticky Clients und 802.11r/k/v**
- **10.10 Band Steering, Load Balancing und Clientfähigkeiten**
- **10.11 Versteckte SSID, Captive Portal und Client Isolation**
- **10.12 VLAN-Zuordnung, AP-Uplink und PoE**
- **10.13 AP- und Controllerauslastung, Treiber, Firmware und Energiesparen**
- **10.14 Systematischer WLAN-Diagnoseablauf**

Kapitel 11 – WAN, Internet, VPN und Remotezugriff

- **11.1 Provider, Modem, ONT und PPPoE**
- **11.2 Öffentliche IP-Adresse, CGNAT und Erreichbarkeit von außen**
- **11.3 WAN-Latenz, Jitter, Paketverlust, Bandbreite und QoS**
- **11.4 Site-to-Site-VPN und vollständiger Tunnelpfad**
- **11.5 IKE Phase 1, Identität, PSK und Zertifikate**
- **11.6 IPsec Phase 2, Proposal, Cipher, Hash, DH und PFS**
- **11.7 UDP 500/4500, ESP, NAT-T, DPD und Rekey**
- **11.8 Traffic Selectors, überlappende Netze, Tunnelroute und Rückroute**
- **11.9 Client-VPN, Split Tunnel und Full Tunnel**
- **11.10 VPN-DNS, DNS-Suffix, MTU und MSS**
- **11.11 Benutzerberechtigung, MFA, Conditional Access und Clientprofil**
- **11.12 RDP, SSH und WinRM über entfernte Netze**
- **11.13 Systematischer Diagnoseablauf für WAN und VPN**

Kapitel 12 – Windows-Clients

- **12.1 Systemzustand, Version, Architektur und letzte Änderungen erfassen**
- **12.2 Start-, Anmelde- und Benutzerprofilprobleme**
- **12.3 Prozesse, Dienste, Autostarts und geplante Aufgaben**
- **12.4 CPU, Arbeitsspeicher, Paging und Datenträgerauslastung**
- **12.5 Treiber, Geräte-Manager und Energiesparfunktionen**
- **12.6 Windows Update und ausstehende Neustarts**
- **12.7 Systemdateien, DLLs, Registry und Anwendungsabhängigkeiten**
- **12.8 Lokale Gruppen, NTFS-Rechte und effektive Berechtigungen**
- **12.9 Antivirus, EDR, Firewall, Proxy und Zertifikatsspeicher**
- **12.10 BitLocker und TPM**
- **12.11 Drucker, Spooler, Warteschlangen und Treiber**
- **12.12 DNS-, Winsock- und Netzwerkstackprobleme**
- **12.13 Anwendungsabsturz, Bluescreen, LiveKernelEvent und Speicherabbild**
- **12.14 Systematischer Diagnoseablauf für Windows-Clients**

Kapitel 13 – Windows Server, Active Directory und Identität

- **13.1 AD-Rollen, Standorte, Domänen und Abhängigkeiten**

- **13.2 Domain Controller Locator und AD-DNS**
- **13.3 DCDiag, Erreichbarkeit, Advertising und Dienste**
- **13.4 AD-Replikation, Replikationslatenz und Objektprobleme**
- **13.5 SYSVOL, NETLOGON und DFS-R**
- **13.6 FSMO-Rollen und Global Catalog**
- **13.7 Secure Channel, Trust und Computerkonto**
- **13.8 Benutzerkonto, Kennwort, Sperre und Ablauf**
- **13.9 Kerberos-Tickets, SPN und Delegation**
- **13.10 LDAP, LDAPS und Zertifikate**
- **13.11 Gruppenmitgliedschaften und Zugriffstoken**
- **13.12 GPO-Verarbeitung, Priorität, Vererbung und Filter**
- **13.13 Logon Scripts, Laufwerkszuordnungen und SYSVOL-Zugriff**
- **13.14 AD-Datenbank, Speicherplatz und Replikationsqueues**
- **13.15 Systematischer Diagnoseablauf für Active Directory**

Kapitel 14 – macOS-Clients

- **14.1 macOS – Prozesse, Dienste, Logs und Ressourcen diagnostizieren**
- **14.2 App-Start, Hänger, Abstürze, Sample und Spindump**
- **14.3 launchd, LaunchAgents und LaunchDaemons**
- **14.4 Unified Logging, Konsole, Crash- und Panic-Berichte**
- **14.5 CPU, Speicherdruck, Komprimierung und Swap**
- **14.6 APFS, Datenträger, Snapshots und Speicherplatz**
- **14.7 Unix-Berechtigungen, ACLs, Dateiflags und erweiterte Attribute**
- **14.8 TCC, Datenschutzfreigaben und geschützte Ressourcen**
- **14.9 Gatekeeper, App-Signatur und Quarantäne**
- **14.10 Anmeldeobjekte, Hintergrunddienste und Systemerweiterungen**
- **14.11 Netzwerk- und externe Abhängigkeiten von Apps**
- **14.12 Sicherer Modus, Apple Diagnose und macOS-Wiederherstellung**
- **14.13 Systematischer Diagnoseablauf für macOS-Clients**

Kapitel 15 – Datei-, Freigabe-, Rechte- und Druckdienste

- **15.1 SMB-Erreichbarkeit, DNS und TCP 445**
- **15.2 Freigaberechte, NTFS-Rechte und effektiver Zugriff**
- **15.3 Gruppen, Access-Based Enumeration, Kerberos, NTLM und SPN**
- **15.4 DFS Namespace, DFS-R und Offline Files**
- **15.5 Dateisperren, Pfade, Zeichen, Quotas und voller Datenträger**
- **15.6 Eigentümer, ACLs, SMB-Version und Signing**

- **15.7 Netzwerkdrucker, TCP/IP-Port, DNS und SNMP-Status**
- **15.8 Spooler, CUPS, Warteschlangen, Treiber und Druckrechte**
- **15.9 Papier-, Toner-, Mechanik- und Gerätestörungen**
- **15.10 Systematischer Diagnoseablauf für Datei- und Druckdienste**

Kapitel 16 – Linux-Server

- **16.1 Systemzustand, Distribution, Kernel und letzte Änderungen erfassen**
- **16.2 systemd Units, Abhängigkeiten und Startreihenfolge**
- **16.3 Konfigurationssyntax, Ports und Listener**
- **16.4 Benutzer, Gruppen, Dateirechte und ACLs**
- **16.5 SELinux und AppArmor**
- **16.6 Pakete, Repositories, Bibliotheken und Abhängigkeiten**
- **16.7 Kernel, Treiber, Prozesse, OOM Killer und Hänger**
- **16.8 CPU, Load, Arbeitsspeicher und Swap**
- **16.9 Dateisysteme, Inodes, Mounts und Read-only-Zustände**
- **16.10 LVM, RAID, I/O-Wait und Datenträgerleistung**
- **16.11 DNS, Routing, Policy Routing und Firewall**
- **16.12 Cron, systemd Timer, Logrotation und Zeitdienste**
- **16.13 SSH, Schlüssel, Berechtigungen und Zugriffsregeln**
- **16.14 Systematischer Diagnoseablauf für Linux-Server**

Kapitel 17 – Virtualisierung, Cluster und Hochverfügbarkeit

- **17.1 Hypervisor, virtuelle Maschine und Ressourcenpfad**
- **17.2 Managementdienste und nicht startende virtuelle Maschinen**
- **17.3 CPU-Überbelegung, CPU Ready, NUMA und CPU-Pinning**
- **17.4 RAM-Überbelegung, Ballooning, Swapping und Memory Pressure**
- **17.5 Datastore, Thin Provisioning, Storage-Latenz und volle Speicherpools**
- **17.6 Snapshots, Consolidation und gesperrte virtuelle Festplatten**
- **17.7 Virtuelle Switches, Bridges, VLANs, Teaming und virtuelle MAC-Adressen**
- **17.8 Hypervisor-Tools und konkurrierende Zeitsynchronisation**
- **17.9 Live Migration und gemeinsamer Speicher**
- **17.10 Quorum, Witness und Split Brain**
- **17.11 HA, Failover, Fencing und STONITH**
- **17.12 Replikation, Backupbelastung und systematischer Diagnoseablauf**

Kapitel 18 – Docker, Container und Kubernetes

Kapitel 19 – Storage, RAID, NAS, SAN und Backup

Kapitel 20 – Web, API, TLS, Reverse Proxy und Load Balancer

- **20.1 Vollständiger Web- und API-Anfragepfad**
- **20.2 DNS, TCP 80/443, Listener und Zielerreichbarkeit**
- **20.3 Zertifikatsgültigkeit, Hostname, SAN, Kette und CA**
- **20.4 TLS-Version, Cipher, SNI, OCSP und CRL**
- **20.5 Reverse Proxy, Zielhost, Zielport, Header und Redirects**
- **20.6 HTTP 400, 401, 403, 404, 405, 408 und 429**
- **20.7 HTTP 500, 502, 503, 504, Backends und Timeouts**
- **20.8 Load-Balancer-Healthchecks und Session Persistence**
- **20.9 API-Key, OAuth, Token und Clientzertifikat**
- **20.10 Cookies, SameSite, Secure, CORS und WebSocket**
- **20.11 Größenlimits, Uploadlimits, Rate Limits und Verbindungsgrenzen**
- **20.12 Cache, CDN, WAF und Anwendungsprotokolle**
- **20.13 Systematischer Diagnoseablauf für Web und API**

Kapitel 21 – Datenbanken, Queues und Backenddienste

- **21.1 Host, Port, Datenbankname, DNS und Firewall**
- **21.2 Zugangsdaten, Secrets, TLS und Netzwerkberechtigungen**
- **21.3 Connection Pool und maximale Verbindungen**
- **21.4 Langsame Abfragen und fehlende Indizes**
- **21.5 Locks, Deadlocks und lange Transaktionen**
- **21.6 Replikationsverzug und Read-only-Replikate**
- **21.7 Storage-Latenz, Transaction Log, WAL und Temp-Bereich**
- **21.8 Schema, Migration, Zeichensatz und Collation**
- **21.9 Backups und blockierende Wartungsjobs**
- **21.10 Message Queues, Consumer, Poison Messages und Retry Storms**
- **21.11 Cache-Dienste und veraltete Cache-Inhalte**
- **21.12 Systematischer Diagnoseablauf für Backenddienste**

Kapitel 22 – E-Mail, Collaboration und Cloud/SaaS

- **22.1 SMTP-Pfad, Ports und Smarthost**
- **22.2 SMTP-Authentifizierung, TLS, Relay, Queue und Empfängerfehler**
- **22.3 MX, SPF, DKIM, DMARC und Reverse DNS**
- **22.4 Spam, Quarantäne, Transportregeln und Größenlimits**
- **22.5 Postfach, Lizenz, Quota, Freigabe und Kalenderberechtigungen**
- **22.6 Service Health, Cloudregion und SaaS-Endpunkte**

- **22.7 Tenant, Rollen, IAM, Conditional Access und MFA**
- **22.8 Token, Sitzung und veraltete Authentifizierung**
- **22.9 API-Quotas und Cloud-Limits**
- **22.10 Security Groups, NSG, NACL, Route Tables und Cloud-Firewall**
- **22.11 Private Endpoints, Private DNS und Proxyzugriff**
- **22.12 Systematischer Diagnoseablauf für E-Mail und Cloud/SaaS**

Kapitel 23 – Performance und „alles ist langsam“

- **23.1 Leistung objektiv messen und Baselines verwenden**
- **23.2 Clientzeit, Netzwerkzeit, Serverzeit und Backendzeit trennen**
- **23.3 CPU-Sättigung, Single-Thread-Limit und Scheduling**
- **23.4 RAM-Druck, Paging, Swapping und NUMA**
- **23.5 I/O-Wait, Datenträgerlatenz und Queue Depth**
- **23.6 Latenz, Jitter, Paketverlust, Durchsatz und Retransmissions**
- **23.7 Speed, Duplex, Oversubscription, Queue Drops und Microbursts**
- **23.8 WLAN-Airtime, Signal, SNR und Kanalauslastung**
- **23.9 DNS-, Proxy- und TLS-Latenz**
- **23.10 Anwendung, Connection Pool, Datenbanklocks und Queues**
- **23.11 Backups, Scans, Wartungsjobs, Snapshots und Logging Storms**
- **23.12 Browser, Add-ons, Antivirus und lokale Clientleistung**
- **23.13 Lastverteilung, synthetische Messungen und APM**
- **23.14 Intermittierende Leistungsfehler und gemeinsame Timeline**
- **23.15 Systematischer Diagnoseablauf für Performanceprobleme**

Kapitel 24 – Security-Vorfälle und verdächtiges Verhalten

- **24.1 Security-Verdacht erkennen und Beweise vor Veränderungen sichern**
- **24.2 Ungewöhnliche Anmeldung, Brute Force und Password Spray**
- **24.3 Kontoübernahme, Administratorkonten und Gruppenänderungen**
- **24.4 Verdächtige Prozesse, Autostarts und PowerShell-Aktivität**
- **24.5 Malware- und Ransomware-Verdacht**
- **24.6 Ungewöhnlicher Netzwerkverkehr, DNS-Tunneling und Datenabfluss**
- **24.7 Rogue DHCP, Rogue DNS und unbekannte Access Points**
- **24.8 Unerwartete Ports, manipulierte Dateien und deaktivierte Schutzsysteme**
- **24.9 Loglöschung, kompromittierte Zertifikate, Secrets und Cloudtokens**
- **24.10 Triage, kontrollierte Isolation und Eindämmung**

Kapitel 25 – Monitoring, Alarmierung und Dokumentation

Kapitel 26 – Spezialdienste

Kapitel 27 – Schnellreferenzen und Runbooks

Verbindliche Fortsetzungsregel

Die Ausarbeitung erfolgt ausschließlich in der Reihenfolge dieser Übersicht. Nach einer fertiggestellten Seite folgt immer die unmittelbar nächste vorhandene Nummer. Existiert in einem Kapitel keine weitere Seite, beginnt das nächste Kapitel mit `.1`.

Beispiel für den Übergang von Kapitel 8 zu Kapitel 9:

`8.3 → 8.4 → 9.1`

Nicht zulässig ist:

`8.3 → 8.4 → 8.5`

Eine Änderung dieser Übersicht ist nur dann gültig, wenn zuerst dieses Referenzdokument vollständig aktualisiert wird. Eine spontan erzeugte Seite verändert die Inhaltsübersicht nicht.
