TrueNAS

Das umfassende Praxisbuch

Franz Claus

Ein Blick ins Buch.

Inhaltsverzeichnis und Einstieg aus der ersten Auflage.
Die folgenden Seiten sind ein Auszug aus der Druckdatei.
Die Seitenzahlen des Buchs bleiben erhalten.

Inhaltsverzeichnis

Teil 1: Einstieg, Grundlagen und Orientierung 10
1.1 Vorwort 10
1.2 Über dieses Buch 11
1.3 Zielgruppe 12
1.4 Lernpfade 13
1.5 Typografische Konventionen 13
1.6 Sicherheit, Haftung und Arbeitsweise 14
1.7 Buchaufbau 15
1.8 Einleitung 17
1.8.1 Schneller Praxispfad: Ein erster sinnvoller TrueNAS-Server 17
1.8.2 Erster Aufbau: vom leeren Server zur funktionierenden *SMB*-Freigabe 18
1.9 Grundlagen und Geschichte 21
1.9.1 Historie von *ZFS* und TrueNAS 21
1.9.2 Philosophie und Zielgruppen 22
1.9.3 Der Aufbau dieses Buchs 25
1.10 Versionskompass: Electric Eel, Fangtooth und Goldeye 26
Teil 2: Hardware, Installation und Erstkonfiguration 28
2.1 Hardware und Installation im Detail 28
2.1.1 Hardware-Planung - mehr als nur Platten 28
2.1.2 Installation im Detail 36
Teil 3: Storage mit *ZFS* in der Praxis 41
3.1 *ZFS* im Detail 41
3.1.0 ZFS in wenigen Minuten 41
3.1.1 *ZFS*-Design - unter der Haube 42
3.1.2 *Vdev*-Typen und RAID-Strategien 43
3.1.3 *Datasets* und Properties 47
3.1.4 *Snapshots*, Klone und *Replikation* im Detail 54
3.1.5 *Boot-Environments*, Upgrades und Rollbacks 63
3.1.6 Performance-Tuning und RAM-Caches 64
3.1.7 Fehlertoleranz und Wiederherstellung 72
Teil 4: Zugriff auf Daten: Netzwerk, Freigaben und Rechte 77
4.1 Netzwerkgrundlagen und Transport 77
4.1.0 Begriffskompass: Protokolle und Netzwerkbegriffe 77
4.1.1 Netzwerkgrundlagen: Schnittstellen, LACP, VLANs und MTU 78
4.1.2 High-Performance Networking - Datacenter 81
4.2 Freigabeprotokolle 86
4.2.1 SMB - Windows- und macOS-Freigaben 86
4.2.2 NFS - Unix-Freigaben 91
4.2.3 iSCSI - Blockspeicher über IP 91
4.2.4 S3, WebDAV, FTP und andere Dienste 93
4.3 Benutzer, Gruppen, ACLs und Identity Mapping 95
4.3.1 Lokale Benutzer und Gruppen 95
4.3.2 Verzeichnisdienste - AD, LDAP und Kerberos 96
4.3.3 ACLs - Rechte sauber planen und anwenden 97
4.3.4 ACL-Universum - NFSv4, ZFS-Properties, CLI und Diagnose 108
4.3.5 Enterprise Identity Mapping (AD-Integration) 116
Teil 5: Apps, Virtualisierung, Betrieb und Sicherheit 121
5.1 Virtualisierung, Apps und Container 122

5.1.1 Virtuelle Maschinen im Detail ... 122
5.1.2 Apps und Container: Kubernetes historisch, Docker Compose aktuell ... 124
5.1.3 Jails und Plugins in *TrueNAS CORE* ... 127
5.1.4 CI/CD und Runner: historisch Kubernetes, aktuell Docker ... 128
5.2 Datensicherung, Monitoring und Wartung ... 129
5.2.1 Backup-Strategien - 3-2-1-Regel ... 129
5.2.2 Monitoring und Reporting ... 133
5.2.3 Wartung und Updates ... 134
5.2.4 S.M.A.R.T-Tests und *Scrubs* ... 134
5.3 Hochverfügbarkeit und Skalierung ... 137
5.3.1 HA-Appliances und Dual-Controller ... 137
5.3.2 SCALE-Cluster - Scale-Out und Hyperconvergence ... 138
5.3.3 Replikations- und Disaster Recovery ... 138
5.4 Sicherheit und Compliance ... 139
5.4.1 Verschlüsselung ... 139
5.4.2 Netzwerksicherheit ... 143
5.4.3 Zugriffskontrolle und Audit ... 143
5.4.4 Datenschutz und Compliance ... 143
5.5 Troubleshooting und Best Practices ... 149
5.5.1 Häufige Fehler und deren Behebung ... 149
5.5.2 Best-Practices ... 150
5.5.3 Community, Support und Weiterbildung ... 150
Teil 6: Expertenwissen: *ZFS*, Recovery und Netzwerk-Engineering ... 152
6.1 *ZFS*-Internals, Topologien und Forensik ... 152
6.1.1 *ZFS*-Topologien und Internals für Profis ... 152
6.1.2 *ZFS*-Architektur - Metaslabs, *ZIL* und *dRAID* ... 157
6.1.3 *ZFS*-Forensik und Metaslab-Management ... 168
6.1.4 Die Mathematik der Speicherplanung ... 176
6.2 Performance, Shell-Troubleshooting und Disaster Recovery ... 180
6.2.1 Performanceanalyse und Tuning ... 180
6.2.2 Troubleshooting auf Shell-Ebene ... 182
6.2.3 Forensik & High-End Troubleshooting ... 182
6.2.4 Extreme Disaster Recovery - Wenn nichts mehr geht ... 184
6.3 Netzwerk-Engineering, *RDMA* und *PFC* ... 189
6.3.1 Netzwerk-Engineering über *LACP* hinaus ... 189
6.3.2 Lossless Networking - *RDMA* & *PFC* ... 191
Teil 7: Automatisierung, Virtualisierung für Profis und erweiterte Administration ... 197
7.1 Automatisierung, *API* und Middleware ... 197
7.1.1 API-Zugriff, midclt und Middleware-Grundlagen ... 197
7.2 Virtualisierung für Profis und Storage-Latenz ... 222
7.2.1 Virtualisierung für Profis - Passthrough & SR-IOV ... 223
7.2.2 Virtualisierung & GPU-Passthrough ... 224
7.2.3 Virtualisierung & Storage-Latenz ... 225
7.3 Enterprise-Sicherheit, *KMIP*, *SEDs* und Compliance ... 227
7.3.1 Unternehmens-Sicherheit - *KMIP*, Self-Encrypting Drives und Compliance ... 228
7.4 Weitere Administrationsthemen ... 230
7.4.1 *USV*, *2FA*, Zertifikate, *TRIM* und Boot-Recovery ... 230
Teil 8: Praxisrezepte, Quellen und Abschluss ... 258
8.1 Fallstudien und Praxisrezepte ... 258
8.1.1 Mediaserver mit Plex und *ZFS*-Storage ... 259
8.1.2 Nextcloud-Hosting für ein kleines Büro ... 260
8.1.3 Unternehmens-Backup über *iSCSI* ... 261

8.1.4 Eigene Apps betreiben: historisch Kubernetes, aktuell Docker Compose 262
8.1.4a Homelab-App-Beispiele: Immich, Jellyfin und Paperless-ngx 263
8.1.5 Automatisiertes Offsite-Backup mit *Cloud Sync* 263
8.2 Glossar: Fachbegriffe im Überblick 268
8.3 TrueNAS-Beginner-Kompass 298
8.4 Quellen und weiterführende Literatur 299
8.4.1 Quellen und weiterführende Dokumentation 300
8.5 Ausblick: Zukunft von TrueNAS und Storage-Hardware 308
8.5.1 Versionsstand dieses Buchs 309
8.5.2 Was 2025 gekommen ist: Fangtooth und Goldeye 309
8.5.3 Was TrueNAS 26 bringt - offiziell sichtbar, aber mit Beta-Vorsicht 310
8.5.4 Hardware-Trends: größere Datenträger, schnellere Netze und KI-GPUs 311
8.5.5 Was das praktisch für Ihre Planung heißt 312
8.5.6 Wo Sie aktuell bleiben 313
8.6 Epilog 314
Anhang A: Architekturdiagramme und visuelle Orientierung 315
Anhang B: Kommandoreferenz für den Betrieb 318
B.1 *ZFS*- und *Pool*-Befehle 318
B.2 *Dataset*-, *Snapshot*- und Replikationsbefehle 319
B.3 *SMB*, *ACL* und Identitätsprüfung 319
B.4 midclt und API 320
Anhang C: Ausgearbeitete Praxisrezepte 321
C.1 Kleiner *SMB*-Dateiserver mit Gruppenrechten 321
C.2 Offsite-*Replikation* mit verschlüsseltem Raw-Send 322
C.3 VM-/*iSCSI*-Storage mit *Zvol* und *Volblocksize* 322
C.4 Migration von TrueNAS CORE zu TrueNAS SCALE/Community Edition 323
Anhang D: Expertenvertiefungen 325
D.1 Enterprise-*ZFS*-Design-Review: Architektur vor Befehlen 325
D.1.1 Reviewablauf und Artefakte 326
D.2 Property-Atlas für Experten: Wirkung, Risiko und Testmethode 327
D.2.1 Property-Änderungen als Change-Prozess 328
D.3 Speicherplanung mit Zahlen: Kapazität, IOPS, Latenz und Wiederherstellungszeit 329
D.3.1 Näherungsrechnungen richtig verwenden 330
D.4 *dRAID*, *RAIDZ* und *Mirrors*: Produktionsdesign statt Prospektrechnung 331
D.4.1 *dRAID*-Labor: was vor Produktion gemessen werden muss 332
D.5 Metaslabs, Space Maps und Allokator: Fragmentierung diagnostizieren 332
D.5.1 Metaslab-Ausgaben interpretieren 333
D.6 *zdb*, DVA und Block-Pointer-Forensik: lesen, ohne den Patienten zu zerlegen 334
D.6.1 *zdb*-Leseschule: von Ausgabe zu Hypothese 335
D.7 RDMA/PFC-Netzwerkengineering: Design, Validierung und Gegenbeweise 336
D.7.1 RDMA/ PFC-Fehlerbilder und Gegenproben 337
D.8 VMware, *iSCSI*, *Zvols* und *VAAI*: Blockgrößen sauber auseinanderhalten 337
D.8.1 *VAAI*- und *iSCSI*-Validierung nach Änderungen 339
D.9 CLI, *API* und midclt: wiederholbar, sicher, prüfbar 339
D.9.1 Idempotente Betriebsabläufe 340
D.10 Performance-Runbook und Failure-Playbooks: Diagnose in Reihenfolge 341
D.10.1 Playbook-Schablone 342
D.11 Backup, DR, Sicherheit und Compliance: Wiederherstellung beweisen 343

D.11.1 DR-Übung und Schlüsselkontrolle 344
D.12 Review-Checkliste und Grenzen dieser Referenz 344
Anhang E: Sachregister 346

Teil 1: Einstieg, Grundlagen und Orientierung

1.1 Vorwort

Dieses Buch ist als Begleiter gedacht, es soll nicht jede offizielle Dokumentationsseite ersetzen, sondern Zusammenhänge herstellen: Warum ein *Mirror* anders skaliert als *RAIDZ*, warum *Snapshots* keine vollständigen *Backups* sind, warum *SMB*-Rechte aus mehreren Ebenen bestehen und warum ein Recovery-Plan vor dem Ausfall geschrieben wird, nicht danach.

Es ist aus einem praktischen Ziel entstanden, TrueNAS nicht nur zu bedienen, sondern wirklich zu verstehen. Viele Anleitungen zeigen, wo man klicken muss. Dieses Praxisbuch erklärt zusätzlich, warum eine Einstellung sinnvoll ist, wann sie gefährlich wird und wie man Fehler systematisch findet, statt Einstellungen nur auszuprobieren. Dieses Buch soll dafür eine verlässliche Orientierung bieten.

Der Anspruch ist bewusst hoch: Es geht um Storage-Planung, *ZFS*, Rechtekonzepte, SMB/*NFS*, Virtualisierung, Netzwerkdesign, *Automatisierung*, Forensik und Wiederherstellung. Deshalb sind die Kapitel mit Lernpfad-Markierungen versehen und schwierige Themen werden zuerst einfach eingeordnet, bevor sie technisch tiefer gehen.

Im Laufe dieses Buches werden Ihnen immer wieder kursiv gesetzte Fachbegriffe begegnen, zum Beispiel *Snapshot*, *Vdev* oder *Pool*. Diese Begriffe werden im Glossar in Kapitel 8.2 ab Seite 245 erklärt. Sollten sie nach einzelnen Fachbegriffen suchen werden Sie im Anhang E: Sachregister ab Seite 306 fündig.

> **Leitgedanke:**
> Ein gutes Storage-System ist nicht das System mit den meisten Funktionen, sondern das System, dessen Verhalten Sie auch im Fehlerfall erklären können.

> **Hinweis:**
> Dieses Buch wiederholt Sicherheitsprinzipien ganz bewusst: Snapshots sind kein Backup, ein Restore-Test zählt mehr als ein grüner Backup-Job, Konfigurationssicherungen gehören vor größere Änderungen, und *ACL*-Operationen brauchen immer einen Rückweg. Diese Punkte tauchen mehrfach auf, weil sie in der Praxis genau dort Daten retten, wo hübsche Annahmen versagen.

> Ein gutes technisches Buch darf nicht nur korrekt sein; es muss auch den Moment erkennen, in dem ein Leser vermutlich hängen bleibt. Gerade bei Storage passiert das selten an der Stelle, an der die Oberfläche einen Fehler meldet. Es passiert früher: bei einer falschen Annahme über Redundanz, bei einer zu optimistischen Poolplanung oder bei einem Rechtekonzept, das im Kopf einfach aussieht und in der Praxis wie ein schlecht gelaunter formaler Freigabeschritt funktioniert.

1.2 Über dieses Buch

> **Kernaussage:**
> Lesen Sie technische Kapitel nicht wie einen Roman, sondern wie eine Werkstattkarte: erst Überblick, dann konkrete Aufgabe, dann Prüfung am Testsystem.

Sie müssen dieses Buch nicht linear lesen, auch wenn die Struktur genau dafür geeignet ist. Wer ein neues System plant, beginnt mit Hardware, *Pool*-Design und *Datasets*. Wer ein bestehendes System retten muss, springt zu *Backup*, *Boot-Environments*, *zpool status, zdb* und Disaster Recovery. Wer Rechteprobleme lösen will, liest zuerst *SMB*, dann *ACLs*, dann *idmap*. Das ist keine Schwäche der Struktur, sondern der Versuch, echte Arbeit abzubilden.

Viele Kapitel enthalten bewusst mehrere Ebenen: zuerst die einfache Erklärung, dann die operative Umsetzung und danach die technische Vertiefung. So können Einsteiger mitkommen, ohne dass erfahrene Administratoren nach zwei Seiten innerlich kündigen.

Dies hier ist als Lernbuch und Nachschlagewerk gedacht. Es richtet sich an Leser mit technischem Grundverständnis: *Netzwerk*, Laufwerke, Benutzerkonten und Weboberflächen sollten keine Fremdwörter sein. Absolute Computer-Einsteiger bekommen bewusst keine Klick-für-Klick-Schulung für jedes Betriebssystem. Wer aber einen Server frisch aufsetzen möchte, erhält eine klare Erstaufbau-Spur und erkennt, welche Spezialthemen zunächst übersprungen werden dürfen.

Auch wenn der Titel dieses Buchs „umfassend“ beinhaltet, bedeutet es in diesem Buch nicht lückenlose Enterprise-Referenz, sondern eine breite, praxisnahe Orientierung für Homelab, anspruchsvolle Privatanwender und kleine Unternehmen. Es ersetzt keine Herstellerdokumentation, keinen Supportvertrag und keine Spezialreferenz zu jedem Detail. Themen wie *RDMA*, *VAAI*, *KMIP*, zdb, *iSCSI*-Tuning oder Enterprise-Identity-Mapping werden so erklärt, dass Sie Risiken und Entscheidungen einordnen können; vollständige Spezialreferenzen bleiben Aufgabe der jeweiligen Projektdokumentation und eigener Tests.

Jedes Kapitel beantwortet drei Fragen:

1. Worum geht es? – Der praktische Zweck des Kapitels.
2. Warum ist es wichtig? – Welche Fehler dadurch vermieden werden.
3. Wie setzt man es um? – Konkrete Befehle, Tabellen, Warnungen und Praxisbeispiele.

Dieses Buch sammelt erweiterte TrueNAS-Menüs, nicht in einem separaten Kapitel. Das wäre als Nachschlagewüste zwar beeindruckend, aber praktisch wenig hilfreich. Stattdessen erklärt jeder Abschnitt die Advanced Options genau dort, wo sie im jeweiligen Ablauf auftauchen: Dataset-Optionen bei Datasets, SMB-Optionen bei Freigaben, Replikationsoptionen bei Data Protection und Netzwerkoptionen im Netzwerkteil.

Wenn ein Dialog eine Schaltfläche „Advanced Options“ anbietet, gilt im Buch immer dieselbe Fragefolge: Was bleibt unverändert? Was muss ich verstehen? Was kann Daten, Rechte, Performance oder Erreichbarkeit beschädigen?

1.3 Zielgruppe

Dieses Buch richtet sich nicht an absolute Computer-Einsteiger ohne technisches Grundverständnis und ist keine vollständige Enterprise-Spezialreferenz. Es ersetzt weder die Herstellerdokumentation noch Supportvorgaben, Labortests oder projektspezifische Freigaben. Spezialthemen wie *RDMA*, *VAAI*, *KMIP*, *zdb*, *API-Automatisierung* und *iSCSI*-Tuning werden eingeordnet, damit Entscheidungen und Risiken nachvollziehbar werden; sie werden nicht bis zum letzten Herstellerparameter durchdekliniert.

Vom Homelab-Enthusiasten mit zwei gebrauchten Servern bis zur Firma, die ihre Buchhaltung, CAD-Dateien oder VM-*Backups* darauf ablegt. Die technischen Grundlagen sind dabei dieselben, aber die Risikotoleranz ist es nicht. Dieses Buch macht deshalb immer wieder deutlich, ob eine Empfehlung für Tests, Homelab, kleine Büros oder produktive Unternehmensumgebungen gedacht ist.

Zielgruppe	Empfohlener Lesepfad	Nutzen
Einsteiger mit Linux-Grundwissen	Einleitung, Hardware, Installation, *Pools*, *Datasets*, *SMB*, Backups	Solides Grundverständnis ohne sofortigen Absturz in Expertendetails
Homelab-Admins	Zusätzlich Apps, VMs, Automatisierung, Monitoring, *Boot-Pool*-Recovery	Saubere, wartbare Umgebung statt historisch gewachsenem Chaos
Storage-Power-User	*ZFS*-Deep-Dives, Metaslabs, *dRAID*, IOPS-Mathematik, Burn-in	Technische Entscheidungen nachvollziehbar planen

Zielgruppe	Empfohlener Lesepfad	Nutzen
Unternehmensumgebungen	AD/*idmap*, *SMB*-Registry, *KMIP*, *PFC/RDMA*, HA, *Replikation*	Professionelle Betriebs- und Migrationskonzepte

1.4 Lernpfade

Der schnellste Weg zu einem stabilen System ist selten der kürzeste Klickpfad. Lesen Sie zuerst die Grundlagen, bauen Sie danach ein kleines Testsystem und zerstören Sie dort absichtlich Dinge: ein *Dataset* mit falscher *ACL*, ein deaktivierter Dienst, ein *Snapshot*-Rollback, ein ersetztes virtuelles Laufwerk. Wer Fehler nur theoretisch kennt, lernt sie im Ernstfall unter Puls kennen. Das ist pädagogisch fragwürdig, aber effektiv.

Damit der Einstieg übersichtlich bleibt, sind die Inhalte in drei Lesestufen gegliedert:

- Grundwissen: Muss jeder verstehen, der TrueNAS betreibt. Dazu gehören Hardware, Installation, *Pools*, Datasets, Benutzer, *SMB*/ *NFS* und *Backups*.
- Praxiswissen: Wichtig für den stabilen Betrieb. Dazu gehören ACLs, Snapshots, *Apps*, VMs, *Monitoring*, *Boot-Environments* und Wiederherstellung.
- Expertenwissen/ Deep Dive: Für Spezialfälle und größere Umgebungen. Dazu gehören Metaslabs, *zdb*, *dRAID*, *PFC*/ *RDMA*, *idmap*-Backends, *API-Automatisierung* und Performance-Mathematik.

Für TrueNAS Einsteiger ist es empfohlen zuerst die Einleitung, Hardware-Planung, Installation, *ZFS*-Grundlagen, Datasets, SMB, Backup und Boot-Recovery zu lesen. Danach können Sie die Deep-Dives als Werkzeugkasten verwenden. Komplexe Spezialthemen können beim ersten Durchgang bewusst übersprungen und später gezielt nachgeschlagen werden.

1.5 Typografische Konventionen

> **Neue Hervorhebungen:**
> In dieser Fassung werden Hinweise bewusst auf wenige wiederkehrende Kategorien reduziert. Leitsatz, Merksatz, Hinweis, Praxis, Vergleich, Einordnung, Warnung und Deep Dive bilden das Grundsystem. Zusätzliche Orientierungssätze werden im Fließtext gehalten, damit die Seite nicht aus Etiketten besteht.

Hervorhebungen wie im Absatz darüber sind Prioritätsmarker, kein Pflichtdurchlauf. Für den ersten Aufbau lesen Sie zuerst Fließtext, Leitsatz/ Merksatz, Achtung und die konkreten Schritte. Praxis-, Hinweis- und Deep-Dive-Absätze können beim ersten Durchgang übersprungen und später gezielt gelesen werden.

Darstellung	Bedeutung
`Befehl`	Shell-Befehl, Pfad, *API*-Methode oder Konfigurationswert
Expert-Warning	Kritischer Hinweis mit Risiko für Datenverlust, Rechteprobleme oder Ausfall
Expert-Tipp	Empfehlung aus der Praxis, meist für bessere Wartbarkeit
Deep Dive	Technischer Abschnitt, der für Einsteiger zunächst übersprungen werden kann
Tabellen	Entscheidungs- und Vergleichshilfen; auf schnelle Orientierung und gute Drucklesbarkeit ausgelegt
Fachbegriff	Kursiv gesetzter Begriff; der Begriff wird im Glossar erklärt.

1.6 Sicherheit, Haftung und Arbeitsweise

> **Leitgedanke:**
> Storage-Administration ist Vertrauensarbeit. Ein Befehl, der in einem Blogbeitrag harmlos aussieht, kann auf dem falschen *Pool* verheerend sein. Dieses Buch nennt deshalb nicht nur Befehle, sondern auch die Bedingungen, unter denen sie sinnvoll sind. Wenn ein Kommando destruktiv sein kann, sollte es zuerst in einer VM oder an einem Testpool ausprobiert werden.

Besonders hilfreich und empfohlen ist ein Änderungsprotokoll zu führen. Notieren Sie Pool-Layout, *Dataset*-Zweck, Freigaben, Gruppen, *Snapshot*-Regeln, Replikationsziele und besondere Tunables. Ein solches Dokument wirkt im Normalbetrieb langweilig. Beim ersten echten Ausfall wird es plötzlich zur schönsten Datei im ganzen Unternehmen.

> **Fehler:**
> Produktive Daten werden als Testmaterial verwendet, weil „es ja nur eine kleine Einstellung ist“. Genau dieser Satz ist vermutlich für einen messbaren Anteil aller Admin-Katastrophen verantwortlich.
> **Vorbeugung:**
> Gefährliche Änderungen zuerst in einer Test-VM oder auf einem Testpool

> durchführen, vor *ACL*-Operationen Snapshots erstellen und vor *Updates* die Konfiguration exportieren.
> **Behebung:**
> Änderungen stoppen, Zustand dokumentieren, Snapshot oder Konfigurationsbackup wiederherstellen und erst danach die eigentliche Ursache untersuchen.

TrueNAS verwaltet Daten, die privat, beruflich oder geschäftskritisch sein können. Deshalb gilt: Vor destruktiven Änderungen werden Snapshots erstellt, Konfigurationen exportiert und Restore-Tests durchgeführt.

Die Beispiele in diesem Buch sind Muster. Namen wie tank, media, users, *backup*, eth0 oder pool müssen immer an die eigene Umgebung angepasst werden. Befehle wie badblocks -w, rekursive ACL-Operationen oder zpool attach dürfen niemals blind kopiert werden. Alle administrativen Eingriffe sollten verstanden, dokumentiert und vorher getestet werden.

1.7 Buchaufbau

> **Hinweis zur Orientierung:**
> Kurze Orientierungssätze nennen zu Beginn eines Abschnitts, welche konkrete Entscheidung oder Fähigkeit Sie daraus mitnehmen sollen. Spezialwissen wird ausdrücklich markiert, damit Einsteiger nicht in Deep-Dive-Themen geraten, bevor der Grundaufbau sitzt.

CLI-Befehle in diesem Buch sollen nicht nur ausgeführt, sondern verstanden werden. Achten Sie deshalb immer darauf, welche Ausgabe ein erfolgreicher oder fehlerhafter Lauf erzeugt und ob ein Befehl produktive Daten verändert.

Das Buch folgt einer linearen Struktur: Grundlagen, Praxis und Deep-Dives sind getrennt, aber logisch aufeinander aufgebaut.

Aufbau in 8 Teilen:

Teil	Inhalt	Zweck
Teil 1	Einstieg, Grundlagen und Orientierung	Vorwort, Zielgruppe, Arbeitsweise, Aktualitätshinweis, Einleitung sowie historische und konzeptionelle Grundlagen.
Teil 2	Hardware, Installation und Erstkonfiguration	Hardwareauswahl, Bootmedien, *HBA*/Controller, Burn-in, Installation und erste Systemabsicherung.

Teil	Inhalt	Zweck
Teil 3	Storage mit *ZFS* in der Praxis	*Pools*, *Vdevs*, *Datasets*, *Snapshots*, *Replikation*, *Boot-Environments*, Performance-Grundlagen und Recovery-Basis.
Teil 4	Netzwerk, Freigaben, Benutzer und Rechte	Netzwerkschnittstellen, Bonds, *VLANs*, *SMB*, *NFS*, *iSCSI*, S3/WebDAV/FTP, Benutzer, Gruppen, *ACLs* und *idmap*.
Teil 5	Apps, Virtualisierung, Betrieb und Sicherheit	Apps, VMs, Container, Backup, Monitoring, Updates, HA, Sicherheit, Compliance, Troubleshooting und Best Practices.
Teil 6	Expertenwissen: *ZFS*, Recovery und Netzwerk-Engineering	*ZFS*-Internals, Metaslabs, Space Maps, *ZIL/SLOG*, *dRAID*, *zdb*, Extreme Disaster Recovery, *RDMA* und *PFC*.
Teil 7	Automatisierung, Virtualisierung für Profis und erweiterte Administration	API, JSON-RPC, midclt, Ansible, Passthrough, SR-IOV, KMIP, SEDs, USV, SNMP, IPMI, TRIM, VAAI und Boot-Recovery.
Teil 8	Praxisrezepte, Glossar, Beginner-Kompass, Quellen und Abschluss	Beispielarchitekturen, Begriffsklärungen, Betriebsregeln, Quellenbasis und abschließende Einordnung

Für den ersten Server reicht als Denkmodell: Laufwerke direkt an *ZFS* geben, *Vdev*-Layout bewusst wählen, *Pool* nicht randvoll schreiben, *Datasets* nach Zweck trennen, Freigaben nur auf passende Datasets zeigen lassen, Rechte über Gruppen vergeben und jeden Zugriff mit einem normalen Testbenutzer prüfen.

Diese Reihenfolge ist keine reine Theorie. Wenn ein Zugriff scheitert, liegt der Fehler nicht automatisch bei der Freigabe. Er kann auf jeder Ebene entstehen: Falscher Benutzer, fehlende Gruppenmitgliedschaft, *Share-ACL*, *Dataset-ACL*, Protokoll, *Netzwerk*, Client-Cache oder ein Dienst, der unter einer anderen Identität läuft. Wer die Ebenen trennt, repariert gezielt statt rekursiv am ganzen Pool herumzuklicken.

Ein Laufwerk ist die physische Hardware. Ein Vdev ist die Redundanzgruppe, etwa *Mirror* oder RAIDZ2. Ein Pool fasst ein oder mehrere Top-Level-Vdevs zu nutzbarem ZFS-Speicher zusammen. Ein Dataset ist darin die Verwaltungsgrenze für Eigenschaften wie *Kompression*, *Recordsize*, Quotas, *Snapshots* und ACL-Typ. Ein Share macht einen Pfad über ein Protokoll wie *SMB*, *NFS* oder *iSCSI* erreichbar. Benutzer, Gruppen und *ACLs* entscheiden schließlich, welche Identität auf welchem Weg was tun darf.