Die schlimmsten Fehler im Umgang mit Proxmox VE und ZFS

Proxmox VE Best Practices – wichtige Tipps für Installation und Betrieb

Hinweis zum Alter des Beitrags: Diese Sammlung ist über mehrere Jahre aus unserer täglichen Arbeit mit **Proxmox VE, ZFS, Backup, Storage und Virtualisierung** entstanden. Einzelne Hinweise stammen daher ursprünglich aus älteren Proxmox-Versionen.

Die grundlegenden Empfehlungen und Erfahrungen sind weiterhin aktuell. Wo sich Proxmox VE technisch weiterentwickelt hat, sollte die jeweilige Konfiguration mit der aktuell eingesetzten PVE-Version abgeglichen werden.

Beim Aufbau einer **Proxmox VE Infrastruktur** gibt es zahlreiche Details, die über eine reine Standardinstallation hinausgehen. Viele Probleme zeigen sich erst im produktiven Betrieb – beispielsweise beim Austausch einer Festplatte, bei ZFS, Backup, Replikation, Updates oder nach einem Boot-Disk-Ausfall.

Die folgenden Punkte basieren auf unseren Erfahrungen aus realen **Proxmox-Installationen und Kundenumgebungen**.

Festplatten und Hardware dokumentieren

Seriennummern der Festplatten dokumentieren

Notiert bei der Installation die **Seriennummern der Festplatten und deren Position in den Einschüben**.

Bei einem späteren Ausfall muss eindeutig erkennbar sein, welche physische Disk zu einem ausgefallenen ZFS-Gerät gehört. Fehlt diese Dokumentation, kann im ungünstigsten Fall eine zusätzliche Prüfung oder sogar ein Herunterfahren des Servers notwendig werden, bevor die richtige Festplatte sicher getauscht werden kann.

Hardware-RAID und ZFS nicht vermischen

Wichtig bei ZFS: Hardware-RAID-Controller sollten nicht dadurch als vermeintlicher HBA verwendet werden, dass für jede einzelne Festplatte ein eigenes RAID0 angelegt wird.

Andere haben mit solchen Konstruktionen schlechte Erfahrungen bis hin zu **Datenverlust** gemacht.

Für ZFS sollte ein geeigneter **HBA bzw. JBOD-Modus** verwendet werden, bei dem ZFS möglichst direkten Zugriff auf die einzelnen Datenträger erhält.

ZFS statt LVM für viele Proxmox-Szenarien

Wir bevorzugen bei unseren Proxmox-Installationen in vielen Fällen **ZFS gegenüber klassischem LVM**.

ZFS bietet unter anderem Prüfsummen, Snapshots, Replikation, Kompression, Mirrors und RAID-Z sowie umfangreiche Möglichkeiten zur Überwachung des Storage.

Das bedeutet allerdings nicht, dass LVM technisch grundsätzlich ungeeignet ist. Die Wahl des Storage-Systems sollte zum jeweiligen Einsatzzweck passen.

RAID-Z für virtuelle Maschinen sorgfältig planen

RAID5/RAID6 bzw. ZFS RAIDZ1 und RAIDZ2 sind nicht automatisch die beste Wahl für Storage mit vielen virtuellen Maschinen.

Bei I/O-intensiven VMs sind Mirrors häufig interessanter. RAID-Z eignet sich dagegen besonders für Workloads, bei denen Kapazität und sequenzielle Zugriffe wichtiger als maximale IOPS sind.

Achtung: Bei ZFS RAIDZ1/RAIDZ2 können Blockgröße, ZVOL-Konfiguration und der Workload erheblichen Einfluss auf Speicherbedarf und Performance haben. Eine unpassende Kombination kann zu deutlichem Overhead führen.

Insbesondere die Einstellungen von **volblocksize**, ZFS-Pool, RAID-Z-Geometrie und VM-Workload sollten deshalb gemeinsam betrachtet werden.

Proxmox Updates und Repositories prüfen

Bei Proxmox VE sollte geprüft werden, welche **Proxmox-Repositories** tatsächlich konfiguriert sind.

Je nach Subscription und gewünschtem Update-Kanal stehen unterschiedliche Repositories zur Verfügung. Wer keine Subscription verwendet, muss darauf achten, dass ein geeigneter Proxmox-No-Subscription-Kanal korrekt konfiguriert ist.

Es reicht nicht aus, lediglich die zugrunde liegenden Debian-Paketquellen zu aktualisieren und davon auszugehen, damit automatisch sämtliche Proxmox-Komponenten aktuell zu halten.

SSH mit Public-Key-Authentifizierung absichern

Für administrative SSH-Zugänge sollte nach Möglichkeit **Public-Key-Authentifizierung** anstelle eines reinen Passwort-Logins verwendet werden.

Zusätzlich sollte geprüft werden, ob Passwort-Login für administrative Benutzer vollständig deaktiviert werden kann.

Proxmox Webinterface mit Zwei-Faktor-Authentifizierung schützen

Ein administrativer Zugang zum **Proxmox VE Webinterface ohne Zwei-Faktor-Authentifizierung (2FA)** erhöht unnötig das Risiko eines Account-Missbrauchs.

Für administrative Konten empfehlen wir daher grundsätzlich die Einrichtung eines zweiten Faktors.

Bootloader und alte Proxmox-Installationen prüfen

Bei älteren Proxmox-Installationen sollte bekannt sein, ob das System über **GRUB oder systemd-boot/EFI** gestartet wird und wie die Boot-Partitionen verwaltet werden.

Insbesondere nach Upgrades über mehrere Proxmox-Versionen sollte kontrolliert werden, ob Kernel, EFI-Systempartitionen und Bootloader korrekt gepflegt werden.

ZFS nicht nur über die Proxmox GUI überwachen

Die Proxmox-Oberfläche allein reicht unserer Erfahrung nach nicht aus, um den Zustand eines produktiven **ZFS-Storage** vollständig zu beurteilen.

Zusätzlich sollten regelmäßig unter anderem folgende Bereiche überwacht werden:

- ZPOOL-Status
- SMART-Werte der Datenträger
- Kapazität und tatsächliche Pool-Auslastung
- ZFS-Fehler und Checksum Errors

- Scrub-Ergebnisse
- SSD-Verschleiß
- Temperaturen
- ARC und Speicherverbrauch

SSD TRIM konfigurieren und überwachen

Bei SSD-basierten ZFS-Systemen sollte die verwendete **TRIM-Strategie** bewusst festgelegt und überprüft werden.

Ob kontinuierliches ZFS-Autotrim oder ein zeitgesteuerter Trim sinnvoller ist, hängt auch von der eingesetzten Hardware und dem Workload ab.

Scrub und TRIM nicht mit Backup-Zeiten kollidieren lassen

Automatische **ZFS-Scrubs, TRIM-Vorgänge und Backups** sollten zeitlich aufeinander abgestimmt werden.

Bei größeren Storage-Systemen können diese Prozesse erhebliche I/O-Last erzeugen. Sie sollten daher möglichst nicht gleichzeitig mit großen Backups oder besonders I/O-intensiven produktiven Arbeiten laufen.

ZFS ARC bewusst dimensionieren

Der **ZFS ARC** verwendet Arbeitsspeicher als Cache. Die optimale Größe hängt stark vom Einsatzzweck des Servers ab.

Ein Proxmox-Host mit vielen virtuellen Maschinen benötigt eine andere Speicheraufteilung als ein dediziertes Storage-System.

Wir empfehlen deshalb, den ARC nicht einfach aufgrund pauschaler Prozentwerte zu dimensionieren, sondern anhand von RAM-Ausstattung, VM-Bedarf, Storage-Größe und tatsächlichem Workload festzulegen und anschließend zu überwachen.

Ausfall einer Proxmox Boot-Disk vorbereiten

Bei gespiegelten Proxmox-Bootlaufwerken reicht es im Fehlerfall nicht immer aus, lediglich die defekte Festplatte physisch zu ersetzen.

Die neue Disk muss passend **partitioniert, in den ZFS-Pool eingebunden und gegebenenfalls wieder bootfähig gemacht** werden.

Der Ablauf für einen Boot-Disk-Ausfall sollte deshalb bereits vor dem Ernstfall dokumentiert und getestet sein.

/etc/pve zusätzlich sichern

Das Verzeichnis `/etc/pve` ist kein gewöhnliches lokales Konfigurationsverzeichnis. Proxmox stellt die Cluster-Konfiguration über **pmxcfs** bereit.

Wichtige Proxmox-Konfigurationen sollten deshalb zusätzlich **regelmäßig und versioniert gesichert** werden.

KVM- und Remote-Konsolen regelmäßig testen

Remote-Konsolen sollten nicht erst getestet werden, wenn der Server nicht mehr über das Netzwerk erreichbar ist.

Wir empfehlen insbesondere:

- Tastaturbelegung und Sonderzeichen beim Login prüfen
- Passwörter mit Sonderzeichen testen
- Browser- und Client-Kompatibilität kontrollieren

- Remote-KVM bzw. IPMI/iLO/iDRAC regelmäßig testen

Eine jährliche Funktionsprüfung kann verhindern, dass die Notfallkonsole ausgerechnet im Ernstfall nicht verwendbar ist.

E-Mail und Benachrichtigungen testen

Ein Proxmox-System sollte wichtige Ereignisse und Fehler zuverlässig melden können.

Die konkrete Einrichtung des Mailversands hat sich über die verschiedenen Proxmox-Versionen weiterentwickelt. Entscheidend ist deshalb weniger die konkrete Versandmethode als ein **regelmäßig getesteter Benachrichtigungsweg**.

Testet insbesondere, ob Warnungen tatsächlich einen Administrator erreichen.

ZFS-Mountpoints und Directory Storage beachten

Vorsicht bei ZFS und Directory Storage: Ein Verzeichnis sollte nicht unkontrolliert als Storage verwendet werden, wenn an dieser Stelle eigentlich ein ZFS-Dataset gemountet werden soll.

Ist das Dataset nicht gemountet und wird das Verzeichnis trotzdem verwendet, können Daten versehentlich auf dem darunterliegenden Dateisystem landen. Mountpoints und Storage-Verfügbarkeit sollten deshalb überwacht werden.

Proxmox ZFS Replication ersetzt keine Backup-Historie

Die integrierte **Proxmox ZFS Replication** ist eine praktische Möglichkeit, VM-Daten auf einen anderen Proxmox-Node zu replizieren.

Eine Replikation ist jedoch **kein Ersatz für ein Backup mit Historie**. Fehler oder unerwünschte Änderungen können ebenfalls repliziert werden.

Für eine belastbare Datensicherung empfehlen wir zusätzlich ein separates Backup-System, beispielsweise **Proxmox Backup Server**.

ZFS Snapshots sinnvoll einsetzen

Regelmäßige **ZFS-Snapshots** sind eine sinnvolle Ergänzung für Storage und Wiederherstellung.

Snapshots benötigen zunächst wenig zusätzlichen Speicher, können bei vielen Änderungen jedoch erheblich wachsen. Die tatsächliche Pool-Auslastung muss deshalb überwacht werden.

ZFS-Pools nicht vollständig füllen: Für produktive Systeme sollte ausreichend freier Speicher vorhanden bleiben. Sehr hohe Pool-Auslastungen können Performance und administrativen Handlungsspielraum erheblich verschlechtern.

Ceph nur mit passender Infrastruktur einsetzen

Ceph ist eine leistungsfähige Lösung für verteilten Storage, aber kein Selbstzweck.

Für kleine Installationen kann ein sauber aufgebautes ZFS-Konzept einfacher, wirtschaftlicher und leichter zu betreiben sein.

Ceph erfordert Erfahrung sowie eine passende Anzahl an Nodes, Datenträgern, Netzwerkbandbreite und Monitoring. Vor einer Ceph-Einführung sollten deshalb Anforderungen und vorhandene Infrastruktur genau geprüft werden.

CPU-Typ virtueller Maschinen bewusst auswählen

Der CPU-Typ einer KVM-VM beeinflusst, welche Funktionen der physischen CPU innerhalb der virtuellen Maschine zur Verfügung stehen.

`host` kann eine hohe CPU-Feature-Abdeckung und Performance ermöglichen. Bei Clustern und insbesondere bei **Live-Migration zwischen unterschiedlichen CPU-Generationen** muss die Auswahl jedoch sorgfältig geplant werden.

Für Cluster kann ein gemeinsamer CPU-Typ sinnvoller sein als pauschal `host` für jede VM zu verwenden.

VirtIO- und Windows-Gasttreiber

Bei produktiven Windows-VMs empfehlen wir, **stabile und getestete VirtIO-Treiber** einzusetzen.

Neue Treiberversionen sollten vor einem flächendeckenden Rollout zunächst getestet werden.

Backups niemals ausschließlich auf dem Proxmox-Host speichern

Ein Backup auf demselben Server ist kein ausreichendes Backup-Konzept.

Backups sollten nicht ausschließlich auf `local` bzw. auf demselben physischen Proxmox-Host gespeichert werden, auf dem die produktiven VMs laufen.

Bei einem Defekt, Dateisystemproblem oder vollständigen Ausfall des Hosts wären ansonsten sowohl Produktivsystem als auch Backup betroffen.

Für produktive Umgebungen empfehlen wir einen getrennten **Proxmox Backup Server oder ein anderes physisch getrenntes Backup-Ziel**.

Video: Proxmox VE Praxistipps

Zu diesen Erfahrungen haben wir auch ein Video veröffentlicht:

Proxmox VE Praxistipps auf YouTube ansehen

Proxmox Tools und Postinstaller auf GitHub

Viele unserer Werkzeuge für Proxmox VE stellen wir als Open Source zur Verfügung. Dazu gehört unter anderem unser **Proxmox VE Post Install Script**.

bashclub – Proxmox Tools und Postinstaller auf GitHub

Stand der Dokumentation: Diese Seite ist aus einer älteren Sammlung unserer Proxmox-Praxiserfahrungen entstanden und wird inhaltlich weiterhin als technische Orientierung gepflegt. Da sich Proxmox VE, Debian, ZFS, Kernel, Bootloader und Hardwareunterstützung weiterentwickeln, sollten konkrete Befehle und versionsabhängige Einstellungen immer gegen die Dokumentation der eingesetzten Proxmox-Version geprüft werden.

Version #2
Erstellt: 2023-05-04 14:15:31 UTC von Christian Zengel (sysops GmbH)
Zuletzt aktualisiert: 2026-07-28 14:12:59 UTC von Christian Zengel (sysops GmbH)