

Backup und Replikation trojanersicher für Proxmox VE mit Miyagi Workflow

Was wir uns Wünschen

“ Für eine Datensicherung wünschen wir uns drei Kopien der Daten an mindestens zwei Standorten, mit zwei Methoden.
Zusätzlich ist die Kontrolle ohne Fehlerquote ein Muss!

Unsere Lösung erzeugt auf einem oder mehreren Systemen

1. Natives Proxmox Backup ohne Löschmöglichkeit auf der Quelle (Restoreversprechen)
2. Natives ZFS Replikat (Restoregarantie)
3. Lückenloses Monitoring ohne Fehlerquote oder Aufwand
4. Serialisierung der Sicherungen für bessere Leistung
5. Automatisierung von Updates, Backupwartung und -verifizierung und Herunterfahren des Sicherungsservers
6. Zentrales Dashboard für Funktion und Sicherung aller Systeme
7. Schnelle Wiederherstellung durch Proxmox Backupserver oder Starten von replizierten Systemen

“ Als Ergebnis finden wir eine Backuphistorie für mehrere Monate bis Jahre und Replikate von ca. 14 Tagen bis drei Monate

Virtual Machine 101 (win.lwnet.local) on node 'lwpve2' No Tags

Start Shutdown Migrate Console More Help

Summary Backup now Restore File Restore Show Configuration Edit Notes Change Protection Remove Storage: backup Filter VMID Search:

Name	Notes	Date ↓	Format	Size	Encrypted	Verify State
vm/101/2025-05-12T16:19:22Z	win.	2025-05-12 16:19:22	win		No	None
vm/101/2025-05-08T10:25:36Z	win.	2025-05-08 10:25:36	win		No	None
vm/101/2025-05-07T03:58:33Z	win.	2025-05-07 03:58:33	win		No	None
vm/101/2025-05-06T12:35:41Z	win.	2025-05-06 12:35:41	pbs-vm	68.72 GB	No	None
vm/101/2025-05-06T12:20:02Z	win.	2025-05-06 12:20:02	pbs-vm	68.72 GB	No	None

Backupansicht in PVE

```
# Auf dem Zielsystem sollte das dann so aussehen
```

```
# Unsere Proxmox Backups mit fünf Tagen Snapshot gegen Kompromittierung
```

```
zfs list
```

```
rpool/pbsstore          4.9T  30.4T  4.62T  /rpool/pbsstore
```

```
#PVE mit LXC Container
```

```
rpool/repl/lwpve2/rpool/data/subvol-100-disk-0  168G  34.8G  165G  /rpool/repl/lwpve2/rpool/data/subvol-100-disk-0
```

```
rpool/repl/lwpve2/rpool/data/subvol-102-disk-0  918M  31.1G  872M  /rpool/repl/lwpve2/rpool/data/subvol-102-disk-0
```

```
#PVE mit KVM
```

```
rpool/repl/lwpve3/rpool3/data/vm-301-disk-0    267K  41.0T  169K  - (finden sich unter /dev/zvol/rpool....)
```

```
rpool/repl/lwpve3/rpool3/data/vm-301-disk-1    40.6G  41.0T  26.7G  - (finden sich unter /dev/zvol/rpool....)
```

```
rpool/repl/lwpve3/rpool3/data/vm-301-disk-2    277G  41.0T  214G  - (finden sich unter /dev/zvol/rpool....)
```

“ Die Backups benötigen für die Wiederherstellung den Zeitpunkt, den Platz und Zeit, während die ZFS Replikate sofort startfähig sind und in Potenter Hardware produktiv gehen können.

Die Aufbewahrungszeiten für Backups und Replikaten können selbst festgelegt werden.

Überlegungen zu Proxmox VE

Proxmox VE ist primär nur ein überschaubares Frontend für KVM und LXC Virtualisierung.

Es ist natürlich denkbar alte VMware- und HyperV Lösungen auf Proxmox umzustellen.

“ Nutzt man Proxmox mit Hardware Raid oder SAN, verliert man im Vergleich zu den kommerziellen Lösungen eine Menge Komfort.

Natürlich ist die Hochverfügbarkeit und das schlanke Design ein Gewinn im Vergleich zu den kostenintensiven Lösungen des Wettbewerbs.

“ Proxmox lebt vor allem durch die im Hintergrund integrierten Lösungen KVM, LXC, SDN und vor allem ZFS und Ceph.

ZFS und Ceph schicken Hardware Raids und SANs auf die Ersatzbank und sind nunmehr oft obsolet.

“ Lösungen mit Ceph werden primär eingesetzt wenn im Härtefall kein Bit Daten verloren gehen darf, was allerdings mit einem vier- bis sechsfachen Kostenaufwand einhergeht.

Mit ZFS erreicht man realistisch eine Sicherung unter fünf Minuten oder besser, wenn notwendig. Nur weil bei einem Server das Licht ausgeht, sind noch lange die Daten nicht weg!!!

Bei eher nicht zu erwartenden Problemen mit einem Ceph Cluster müsste man eventuell von vorne starten.

Kleinere Installationen von ca. ein bis drei Proxmox Servern sollten daher mit ZFS installiert und untereinander repliziert werden.

Die Replikation mit Bordmitteln sieht jedoch nur den Transport und keine Historie der Systeme vor.

Da heutzutage SSDs und Festplatten nicht mehr von vorne bis hinten beschrieben werden, sondern zufällig, macht es Sinn die komplette Lebenszeit den kompletten Platz auszunutzen.

Von Dummheit, Fahrlässigkeit bis zum Trojaner

Vor Umstellungen und Maßnahmen führt der Admin üblicherweise einen Snapshot aus. Gerade VMware ist die absolut im Nachteil gegen die meisten Systeme, da Konsolidierung der Snapshots nach Tagen schon den Betrieb lahmlegen kann. Daher ist eine hohe Anzahl von Snapshots im HyperV und VMware keine Option.

Hier kommt ZFS ins Spiel.

“ Durch die auf Vektoren basierende Arbeitsweise von ZFS sind permanente Snapshots kein Nachteil für den Betrieb.

Wir empfehlen folgende Vorgehensweise.

Installation einer Snapshot Engine wie zfs-auto-snapshot oder CV4PVE (Web GUI für PVE)

Alle Programme inklusive Proxmox VE erstellen dieselbe Qualität an Snapshots, wobei zfs-auto-snapshot von Proxmox unentdeckt arbeitet.

Hierbei ist nur zu beachten, dass das System nicht über 80% belegt wird. Für den Fall der Überlastung können wir die Aufhebezeiten reduzieren.

Unser Vorschlag belegt üblicherweise ca. 2,5 mal so viel Platz wie die Nutzdaten.

Hier die optimalen Einstellungen aus unserer Praxis:

- 12 Snapshots alle 15 Minuten für drei Stunden für schnelle Hilfe
- 96 Stunden für vier Tage, besonders sinnvoll für Ostern, Weihnachten, Krankheit
- 21 Tage für drei Wochen
- 6 Wochen für ein feineres Raster in die Vergangenheit
- 3 Monate für unentdeckte Fehler

Für alles über drei Monate nutzen wir die tägliche Sicherung mit Proxmox Backup Server

Proxmox Backupserver Segen und Fluch

Proxmox Backup Server ist ein ideales Sicherungswerkzeug für virtuelle Maschinen und Linux Container auf Proxmox VE.

Das Design sieht vor daß hier Sicherungen von Proxmox VE nach Proxmox Backupserver geschoben werden, was Raum für Trojaner und Hacker bietet.

“ Es ist extrem wichtig, dem Backupuser im Server einen API Key bereitzustellen, der nur Sicherungs- und Wiederherstellungsrechte besitzt.

Zwei Faktor Login, so wie die Deaktivierung des SSH Logins per Passwort sind absolut notwendig!

Der Backupserver kann nicht wissen wann ein Proxmox VE System seine Sicherung anliefert. Daher muss er permanent laufen.

Selbst ein Anschalten des Backupservers vor der geplanten Sicherung erlaubt ein Herunterfahren nach der Sicherung nicht, da es technisch nicht vorgesehen ist.

Ebenfalls ist das Monitoring der Backups nicht vorgesehen und mit Zabbix oder Check_MK nur mühselig einzurichten.

Die Mailbenachrichtigung ist unzureichend bis unbrauchbar. Ebenfalls fehlt ein Dashboard für Backup, Festplattenzustand oder Raid-Probleme.

Wir benötigen einen weiteren Computer, an einem anderen Ort, mit zwei weiteren Kopien in zwei Methoden der Sicherung

☞ Proxmox VE bietet die Möglichkeit nativ mit dem Backupserver zu sichern und mit ZFS ein startfähiges Replikat nativ zu erstellen.

Backups bieten hier ein **Wiederherstellungsversprechen**, während ZFS eine **Wiederherstellungsgarantie** bietet

Voraussetzungen für den Miyagi Workflow

- Proxmox VE Server 8.4 oder neuer mit ZFS Raid 10 (empfohlen) oder RaidZ (langsamer)
- Optional zfs-auto-snapshot oder CV4PVE Snapshotmanager
- Computer mit möglichst viel Platz, z. B. HPE Microserver mit ECC, 4 x 20TB HDD oder vergleichbare Systeme von Terramaster ohne ECC mit 16 GB RAM (nicht empfohlen)
- Proxmox Backup Server 3.4 oder neuere ISO zur Installation mit ZFS Raid 10 (empfohlen) oder RaidZ (langsamer)
 - Optional alter PC mit Synology iSCSI Freigabe
 - Dafür Cronjob beim booten
 - @reboot iscsiadm --mode node --targetname "iqn.2xxxx" --portal "10.ipsyn...:3260" --login && zpool import -f iscsi
- Bashclub Postinstaller für checkzfs und zsync Tool auf beiden Systemen
<https://github.com/bashclub/proxmox-zfs-postinstall>
- Optional Check_MK Agent auf PVE und PBS

Installation Proxmox Backup und Einstellungen

- PBS: Inhalt von .ssh/id_rsa.pub wird per Web GUI in PVE .ssh/authorized_keys ergänzt
- Einmaliger Login per SSH von PBS zu PVE um den Hostkey zu speichern
- Konfiguration von PBS
 - Kein NFS für PBS nutzen!!!
 - Optional beim booten ein Synology oder ähnliches iSCSI LUN einbinden, falls keine neuen Platten angeschafft wurden
 - Auf der Shell optimierten ZFS Pool und Dataset erstellen, falls nicht nativ installiert wurde
 - Optional mit iSCSI
 - iscsiadm --mode node --targetname "iqn.2xxxx" --portal "10.ipsyn...:3260" --login
 - Bei direkten Platten Raid erstellen
 - zpool create -f iscsi /dev/sdx -o autoexpand=on
 - zfs create iscsi/pbsstore -o recordsize=1M -o com.sun:autosnapshot=false
 - mit lsblk finden wir die Festplatten namen, alternativ unter /dev/disk/by-id (empfohlen=

- Bei nativ installiertem PBS wie folgt den Store anlegen
 - `zfs create rpool/pbsstore -o recordsize=1M -o com.sun:autosnapshot=false`
- In Proxmox Backupserver neuen Store anlegen
 - bei iSCSI nach `/iSCSI/pbsstore`
 - nativ nach `/rpool/pbsstore`
- Purge, Garbage Collection und Verifyjobs anlegen auf 1. Tag im Jahr und deaktivieren, wir regeln das!
- Benutzer `backup@pbs` mit guten Passwort und 2FA anlegen
- API Key `backup@pbs!backup` anlegen, Passwort und Name notieren
- Permission für `"/` Datastore Backup für User `backup@pbs` und API Key `backup@pbs!backup` anlegen.
- In Proxmox VE, also der Quelle
 - Neuen Datastore Typ Proxmox Backup Server

Edit: Proxmox Backup Server

General Backup Retention Encryption

ID: backup DatastorePVE Nodes: All (No restrictions)

Server: 192.168 Enable: ☐

Username: backup@pbs!backup Content: backup

Password: ***** API User und Key Datastore: backup Datastore PBS

Namespace:

Fingerprint aus PBS Titelseite

Fingerprint: 5d:d0:

- Ausführung eines Tests der Datensicherung direkt aus einer VM

“ Achtung: Proxmox VE hat als default den Store "local" auf Typ Backup stehen, dringend deaktivieren!

Installation Miyagi

- Auf Proxmox Backupserver

- `apt install git open-iscsi`
- ```
git clone -b dev https://github.com/bashclub/miyagi-pbs-zfs.git
cd miyagi-pbs-zfs
cp example.conf ipdeinespve.conf
nano ipdeinespve.conf
```

- Miyagi Script sichert einen PVE mit maximal zwei ZFS Pools auf ein Ziel, für mehr einfach mehrere Configs!

`SSHPORT='22' #SSH Port, eventuell extern geändert`

```

BACKUPSERVER=yes #Soll Backup ausgeführt werden
MAINTDAY=6 #1 Montag bis 7 Sonntag, am besten Samstags, da Sonntags Scrubs laufen
SHUTDOWN=yes #Ausschalten nach Beendigung (empfohlen)
UPDATES=yes #Updates PBS

SOURCEHOST='dein pve ip' # IP vom Proxmox VE System das gesichert werden soll

#Replikation mit ZFS
ZFSROOT='rpool/data' Standard ZFS Pool von Proxmox VE mit ZFS
ZFSSECOND='rpool-hdd/data' #Optional zweites ZFS auf HDD
ZFSTRGT='rpool/repl' #Das ist der Proxmox Backup Server mit ZFS installiert

#Falls Sonntags der ZFS Scrub läuft, besser stoppen
ZPOOLSRC=rpool #Erster Pool PVE
ZPOOLDST=rpool #Erster Pool PBS

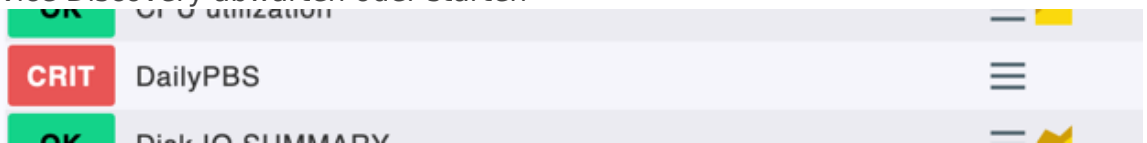
#ZSYNC für ZFS Replication vom github.com/bashclub
ZPUSHTAG=bashclub:zsync #Markiert auf der Quelle mit diesem Wert rekursiv die Datasets
und Volumes
ZPUSHMINKEEP=3 #Standardwert zum Anfügen, nicht ändern
ZPUSHKEEP=14 #Bei täglicher Sicherung wären das 14 Tage!
ZPUSHLABEL=zsync #Name vom Snapshot für die Replikation, dieser muss auf beiden Seiten
erscheinen
ZPUSHFILTER="daily,weekly,monthly" #Falls zfs-auto-snapshot auf Quelle genutzt wird, können
wir diese Snapshots mitnehmen!

#Backup
PBHOST='IPPBS' #IP Adresse des Proxmox Backup Servers
BACKUPSTORE=backup #Datastorename für Backups auf PVE
BACKUPSTOREPBS=backup #Datastorename für Backups auf PBS
BACKUPEXCLUDE='99999' #Weglassen von VMs oder LXCs mit Komma getrennt, nicht leer
lassen!

```

- Danach Testlauf
  - `/root/miyagi-pbs-zfs /pbs-zfs-daily.sh -c /root/miyagi-pbs-zfs/192....conf`
  - Ausgabe sollte Replikation und später Backup anzeigen
  - Shutdown
- Kontrolle Testlauf
  - PBS-Sicherung
    - In Proxmox VE unter Cluster / Datastores den Backup Store wieder aktivieren!

- In den VMs/LXC's oder im Store selbst schauen ob Backups vorhanden sind
- ZFS-Replikation
  - auf PBS in Shell
    - `checkzfs --sourceonly`
    - oder
      - `checkzfs --source ippve --filter rpool/data --threshold 1500,2000 -- columns +message`
  - auf PVE in Shell
    - `cat /var/lib/check_mk_agent/spool/*`
- Check\_MK Monitoring
  - Auf PVE per Service Discovery
  - Service Discovery abwarten oder starten



Zeigt den Status des letzten Backups

|    |                                                                                              |     |                           |
|----|----------------------------------------------------------------------------------------------|-----|---------------------------|
| OK | miyagi-pve-pve232-bashclub:zsync-232-ssd:root@192.168.0.241:22#rpool/data/subvol-1103-disk-0 | ≡ 📁 | rpool/repl/rpool/data/sub |
| OK | miyagi-pve-pve232-bashclub:zsync-232-ssd:root@192.168.0.241:22#rpool/data/subvol-1107-disk-0 | ≡ 📁 | rpool/repl/rpool/data/sub |
| OK | miyagi-pve-pve232-bashclub:zsync-232-ssd:root@192.168.0.241:22#rpool/data/subvol-1120-disk-0 | ≡ 📁 | rpool/repl/rpool/data/sub |
| OK | miyagi-pve-pve232-bashclub:zsync-232-ssd:root@192.168.0.241:22#rpool/data/subvol-1126-disk-0 | ≡ 📁 | rpool/repl/rpool/data/sub |
| OK | miyagi-pve-pve232-bashclub:zsync-232-ssd:root@192.168.0.241:22#rpool/data/subvol-1127-disk-0 | ≡ 📁 | rpool/repl/rpool/data/sub |

Zeigt alle Quelldatasets und -Volumes ohne Fehlerquote, wenn Quelle korrekt angegeben  
 Status geht auf Unknown wenn innerhalb eines Tages keine neuen Daten kommen!

- Ausgeschalteten Miyagi Server kontrollieren
  - Neuen Host mit Namen miyagi-quelle-ziel in Check\_MK anlegen, ohne Agent und API, mit

▼ Basic settings

Hostname ..... miyagi-pve-pve232

Alias ..... ☐ empty (Default value)

Monitored on site ..... ☐

Permissions ..... ☐ empty (Default value)

Parents ..... ☐ empty (Default value)

▼ Network address

IP address family ..... ☐ IPv4 only (Default value)

IPv4 address ..... ☒ 192.168

Additional IPv4 addresses ..... ☐ No entries (Default value)

Additional IPv6 addresses ..... ☐ No entries (Default value)

▼ Monitoring agents

Checkmk agent / API integrations ... ☒ No API integrations, no Checkmk agent

SNMP ..... ☐ No SNMP (Default value)

Piggyback ..... ☒ Use piggyback data from other hosts if present ▼

- Service Discovery abwarten oder starten



Services of Host miyagi-pve-pve232

Monitor > Overview > All hosts > miyagi-pve-pve232 > Services of Host

CommandsHostServicesAdd toExportDisplayHelp

Acknowledge problemsSchedule downtimesFilterShow checkboxesmiyagi-pve-pve232

miyagi-pve-pve232

| State | Service                    | Icons | Summary                                                                                                                                                                                  | Age |
|-------|----------------------------|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| OK    | Check_MK                   |       | [piggyback] Successfully processed from source 'pve.leimeister.com', execution time 0.0 sec                                                                                              | 23  |
| OK    | Check_MK Agent             |       | Version: 2.0.0p24, OS: linux                                                                                                                                                             | 23  |
| OK    | Check_MK Discovery         |       | Services: all up to date, Host labels: all up to date                                                                                                                                    | 23  |
| OK    | Check_MK HW/SW Inventory   |       | Found 6807 inventory entries, hardware changes, Found 24 status entries                                                                                                                  | 23  |
| OK    | CPU load                   |       | 15 min load: 1.30, 15 min load per core: 0.03 (40 cores)                                                                                                                                 | 23  |
| OK    | CPU utilization            |       | Total CPU: 5.17%                                                                                                                                                                         | 23  |
| PEND  | Disk IO SUMMARY            |       |                                                                                                                                                                                          | -   |
| OK    | DISK: sda                  |       | INTEL SSDS...                                                                                                                                                                            | 23  |
| OK    | DISK: sdb                  |       | INTEL SSDS...                                                                                                                                                                            | 23  |
| OK    | DISK: sdc                  |       | INTEL SSDSC2KB019T7 Serial: BTYS8112096V1P9DGN, Size: 1.92 TB, Uptime: 5 years 262 days                                                                                                  | 23  |
| OK    | DISK: sdd                  |       | INTEL SSDSC2KB019T7 Serial: BTYS811306R91P9DGN, Size: 1.92 TB, Uptime: 5 years 262 days                                                                                                  | 23  |
| OK    | DISK: sde                  |       | ST2000NX0253 Serial: W46120Q8, Size: 2.00 TB, Uptime: 5 years 278 days                                                                                                                   | 23  |
| OK    | DISK: sdf                  |       | ST2000NX0253 Serial: W4610MVY, Size: 2.00 TB, Uptime: 5 years 278 days                                                                                                                   | 23  |
| OK    | DISK: sdg                  |       | ST2000NX0253 Serial: W460ZQ8L, Size: 2.00 TB, Uptime: 5 years 278 days                                                                                                                   | 23  |
| OK    | DISK: sdh                  |       | ST2000NX0253 Serial: W460VTD9, Size: 2.00 TB, Uptime: 5 years 278 days                                                                                                                   | 23  |
| OK    | Filesystem /               |       | Used: 3.38% - 40.5 GiB of 1.17 TiB (warn/crit at 91.18%/95.59% used), trend per 1 day 0 hours: +25.3 MiB, trend per 1 day 0 hours: +<0.01%, Time left until disk full: 128 years 91 days | 23  |
| OK    | Filesystem /etc/pve        |       | Used: 0.02% - 20.0 KiB of 128 MiB (warn/crit at 50.00%/72.41% used), trend per 1 day 0 hours: +0 B, trend per 1 day 0 hours: +0%                                                         | 23  |
| OK    | Filesystem /rpool          |       | Used: 77.07% - 3.80 TiB of 4.93 TiB (warn/crit at 93.38%/96.69% used), trend per 1 day 0 hours: +42.1 GiB, trend per 1 day 0 hours: +0.83%, Time left until disk full: 27 days 11 hours  | 23  |
| OK    | Filesystem /rpool-hdd/data |       | Used: <0.01% - 824 KiB of 534 GiB (warn/crit at 89.63%/94.81% used), trend per 1 day 0 hours: -38.2 KiB, trend per 1 day 0 hours: -0.00%                                                 | 23  |

Status offline Server

○

“ Nun können wir den ausgeschalteten Server im Blick behalten. Kommen innerhalb eines Tages keine neuen Daten, geht das System auf Unknown