

Backup and Restore

Purpose

This page documents the backup and restore process for Bytek VMs, LXC's, application data, and configuration.

The current backup system protects against:

- Failed upgrades.
- Broken configuration changes.
- Guest operating-system corruption.
- Accidental deletion.
- Application database damage.
- Failure of a production NVMe disk, provided the backup HDD remains healthy.

The current backup system does not fully protect against:

- Fire.
- Theft.
- Complete host destruction.
- Electrical damage affecting the entire server.
- Compromise of both production and backup storage.
- Failure of the backup HDD before another copy exists.

Backup Storage

Setting	Value
Proxmox storage ID	pve-backup
Mount point	/mnt/pve/pve-backup
Physical disk	/dev/sda

Partition	/dev/sda1
Filesystem	ext4
Approximate capacity	4 TB
Content type	VZDump backup files
Mount protection	Enabled
Current location	Same physical Proxmox server

The backup HDD is dedicated to Proxmox backups.

Do not use the backup HDD for:

- Active VM disks.
 - Nextcloud user data.
 - Plex media.
 - Game-server data.
 - Docker application data.
 - Temporary downloads.
 - General file storage.
-

Mount Validation

Before relying on a backup job, confirm that the backup HDD is mounted.

Use:

```
findmnt /mnt/pve/pve-backup
```

The source should be /dev/sda1.

Check capacity using:

```
df -h /mnt/pve/pve-backup
```

Check Proxmox storage state using:

```
pvesm status
```

The pve-backup storage must show as active.

Mount-point protection prevents Proxmox from writing backup archives into the empty mount directory on the Proxmox root filesystem if the HDD is unavailable.

Scheduled Backup Policy

Setting	Recommended Value
Storage	pve-backup
Compression	ZSTD
General backup mode	Snapshot
Initial application baseline	Stop mode where practical
Selection	All production VMs and LXC's
Notification	Configure for failed jobs

Recommended retention:

Retention Rule	Count
Keep last	3
Keep daily	7
Keep weekly	4
Keep monthly	3

Retention must be adjusted if the backup HDD approaches capacity.

Backup Modes

Snapshot Mode

Use snapshot mode for normal scheduled backups when minimizing downtime is important.

Snapshot mode is appropriate for:

- Infrastructure services.
- Stateless or lightly written services.
- Routine nightly backups.
- Applications with guest-agent filesystem freeze support.

Stop Mode

Use stop mode for the strongest whole-VM consistency when brief downtime is acceptable.

Stop mode is recommended for:

- Initial known-good baselines.
- Database-heavy services before major changes.
- Backups taken before risky upgrades.
- Plex or other VMs with PCI passthrough when snapshot behavior is limited.
- Applications where exact application consistency is more important than continuous availability.

Suspend Mode

Suspend mode is not the preferred mode for the current environment.

QEMU Guest Agent

VMs should have the QEMU Guest Agent enabled.

Check a VM configuration using:

```
qm config <VMID>
```

The configuration should include the guest agent.

Test guest-agent communication using:

```
qm guest cmd <VMID> ping
```

Expected result:

- An empty successful response.

Inside the VM, verify:

```
systemctl is-active qemu-guest-agent
```

Expected result:

- `active`

The guest agent improves guest coordination during snapshot-mode backups.

Disk Inclusion

A VM disk is included in backup by default unless its configuration contains:

```
backup=0
```

Review a VM using:

```
qm config <VMID>
```

Confirm every required operating-system and application-data disk is included.

For Nextcloud, both of these must be included:

- The 64 GB operating-system disk.
- The 500 GB user-data disk.

Large replaceable media disks may eventually be excluded, but only after the exclusion is documented and the application configuration remains protected elsewhere.

Service Backup Coverage

Proxmox Host

The normal guest backup job does not back up the Proxmox host operating system.

Preserve separately:

- `/etc/pve`
- Network configuration.
- Storage configuration.
- Firewall configuration.
- Authentik realm settings.
- Backup-mount configuration.
- VM and LXC inventory.
- Recovery credentials.

WireGuard Gateway

Protect:

- WireGuard configuration.
- Private and public keys.
- Peer definitions.
- Firewall rules.
- NAT rules.
- SSH configuration.
- Network configuration.

Private keys must remain in encrypted storage, not in BookStack.

Pi-hole

Protect:

- Local DNS records.
- DHCP reservations.
- Pi-hole configuration.
- Allow and deny lists.
- Upstream DNS settings.
- LXC network configuration.

A Pi-hole configuration export may supplement the Proxmox backup.

Traefik

Protect:

- `/opt/traefik/compose.yml`
- `/opt/traefik/traefik.yml`
- `/opt/traefik/.env`
- `/opt/traefik/dynamic/`
- `/opt/traefik/data/acme.json`
- Any Basic Auth files.
- Certificate API configuration.

Never delete `acme.json` during normal troubleshooting.

Authentik

Protect:

- PostgreSQL data.
- Redis configuration.
- Compose configuration.
- Environment file.
- Signing keys.
- Applications.
- Providers.
- Policies.
- Groups.
- Outpost configuration.
- Custom templates and media.

PostgreSQL is the authoritative data source for the Authentik configuration.

Uptime Kuma

Protect:

- Persistent `/app/data`.
- Embedded database.

- Monitor configuration.
- Notification configuration.
- Status pages.
- Compose file.
- Uploaded assets.

Nextcloud AIO

Protect:

- 64 GB operating-system disk.
- 500 GB user-data disk.
- AIO master-container configuration.
- PostgreSQL.
- Redis.
- Nextcloud configuration.
- User files.
- Collabora configuration.

The AIO Borg repository is currently unconfigured because no separate backup destination is available.

Vikunja

Protect:

- `/opt/vikunja/postgres`
- `/opt/vikunja/files`
- `/opt/vikunja/config.yml`
- `/opt/vikunja/.env`
- `/opt/vikunja/compose.yml`

BookStack

Protect:

- `/opt/bookstack/app`
- `/opt/bookstack/database`

- `/opt/bookstack/.env`
- `/opt/bookstack/compose.yml`
- BookStack application key.
- Uploaded images and attachments.
- Themes and configuration.

The BookStack application key and database must be restored together.

Application-Level Database Exports

Application-level exports supplement the whole-VM backup.

They do not replace the Proxmox backup.

Vikunja PostgreSQL

Run from `/opt/vikunja`:

```
sudo docker compose exec -T db pg_dump -U vikunja vikunja > vikunja-backup.sql
```

BookStack MariaDB

Run from `/opt/bookstack` using the database service and credentials defined in the Compose environment.

Prompt for the database password rather than placing the password directly in shell history.

Database exports contain sensitive application data.

Store exports securely and remove obsolete copies.

Manual Baseline Backup

Create a manual backup before:

- Major upgrades.
- Authentication changes.
- Database migrations.
- GPU passthrough.
- Major firewall changes.
- Storage changes.
- Disabling a local authentication method.
- Removing an old service.

Example pattern:

```
vzdump <VMID> --storage pve-backup --mode stop --compress zstd
```

Confirm the task ends with:

- TASK OK

List the backup storage using:

```
pvesm list pve-backup
```

Restore-Test Procedure

A backup is not fully trusted until it has been restored and inspected.

1. Select a recent backup.
2. Restore to a new VM or LXC ID.
3. Choose an appropriate target storage.
4. Disconnect the restored guest network adapter.
5. Start the restored guest using the Proxmox console.
6. Confirm the operating system starts.
7. Confirm expected disks are present.
8. Confirm expected filesystems are mounted.
9. Confirm Docker starts.
10. Confirm application containers exist.
11. Confirm the database is available.
12. Confirm persistent application data exists.

13. Shut down the restored clone.
14. Delete the test clone after documenting the result.

Do not start a restored clone on the live LAN while the production guest is active.

The clone may contain the same:

- IP address.
 - Hostname.
 - DHCP identity.
 - Application identity.
 - Database.
 - OIDC configuration.
 - Scheduled tasks.
-

Nextcloud Restore Test

For Nextcloud, confirm:

- The 64 GB OS disk restored.
- The 500 GB data disk restored.
- `/mnt/nextcloud-data` is mounted.
- `/mnt/nextcloud-data/ncdata` exists.
- Docker is active.
- AIO containers exist.
- User data is present.

Keep the network adapter disconnected during inspection.

Backup Monitoring

Monitor:

- Backup job success.
- Backup-HDD mount.

- Backup-HDD free space.
- SMART health.
- Thin-pool usage.
- Backup duration.
- Unexpected backup-size growth.
- Failed guest-agent operations.

Useful checks:

- `pvesm status`
 - `df -h /mnt/pve/pve-backup`
 - `findmnt /mnt/pve/pve-backup`
 - `smartctl -H /dev/disk/by-id/wwn-0x5000cca097c44d7e`
-

Backup-HDD Health

Stable device identifier:

```
/dev/disk/by-id/wwn-0x5000cca097c44d7e
```

Review:

- Overall SMART health.
- Reallocated sectors.
- Pending sectors.
- Offline uncorrectable sectors.
- CRC errors.
- Temperature.
- SMART error log.

Pending or uncorrectable sectors require immediate investigation.

Backup Failure Response

If a backup job fails:

1. Read the Proxmox task log.
2. Confirm `pve-backup` is mounted.
3. Confirm free space.
4. Confirm the guest exists.
5. Confirm all required storage is active.
6. Confirm the QEMU Guest Agent where applicable.
7. Confirm the VM is not locked.
8. Confirm no previous backup task is stuck.
9. Resolve the specific error.
10. Run a manual test backup.
11. Confirm `TASK OK`.
12. Document the failure and correction.

Do not repeatedly rerun a failing job without reading the task log.

Current Limitations

The current backup architecture has two copies:

1. Live production data.
2. Local backup archives on the internal HDD.

Both copies remain:

- In the same physical server.
- In the same building.
- On the same electrical system.
- Under the same administrative control.

A future third copy should use:

- A trusted remote server.
- A dedicated Proxmox Backup Server.
- Encrypted Borg.
- Encrypted Restic.
- Remote PBS synchronization.

- Another physically separate destination.
-

Validation Checklist

- `pve-backup` is mounted.
 - `pve-backup` is active in Proxmox.
 - Backup HDD has sufficient free space.
 - SMART health is acceptable.
 - Nightly backup job is enabled.
 - Retention is configured.
 - Every production guest is included.
 - Required virtual disks are included.
 - Nextcloud OS and data disks are included.
 - Backup-failure notifications are configured.
 - A recent manual backup completed with `TASK OK`.
 - A restored VM was tested offline.
 - Recovery credentials are stored securely.
 - Offsite backup remains documented as outstanding work.
-

Document Control

- **Owner:** Bryan Gagne-Plante
- **Backup storage:** `pve-backup`
- **Mount point:** `/mnt/pve/pve-backup`
- **Physical backup disk:** 4 TB HDD
- **Compression:** ZSTD
- **Routine mode:** Snapshot
- **Baseline mode:** Stop where practical
- **Offsite backup:** Not configured
- **Last verified:** YYYY-MM-DD
- **Last successful scheduled backup:** YYYY-MM-DD
- **Last manual baseline:** YYYY-MM-DD
- **Last restore test:** YYYY-MM-DD
- **Last SMART review:** YYYY-MM-DD

- **Known limitation:** Backup and production storage remain in one physical server

Revision #2

Created 2026-08-17 14:52:33 UTC by Bryan Gagne-Plante

Updated 2026-08-18 00:45:44 UTC by Bryan Gagne-Plante