Backups & Disaster Recovery

First lesson that every homelab journey eventually teaches, it's that it's not a matter of *if* something will break, it's *when*. Especially if you use used hardware from your old computer or cheap mini pc of ebay. Having a solid backup strategy in place before that moment arrives is the difference between a minor inconvenience and losing months of work. This is an area I've been deliberate about, and one that has already proven its worth in a very real way.

Proxmox Backup Server

The backbone of my backup strategy is a dedicated machine running **Proxmox Backup Server (PBS)**. Rather than relying on the Proxmox VE nodes themselves to manage backups, PBS is a standalone system connected to all my PVE environments — giving me a centralized, independent target for all backup jobs.

Every VM and LXC container in the homelab runs on a daily backup schedule. PBS uses a chunk-based, deduplicated storage format, which means it doesn't store a full copy of every VM every day. Instead, it only captures what has changed since the last backup, and deduplicates redundant data across the entire datastore. The result is that daily backups of a full homelab take a fraction of the storage you'd expect. Beyond the scheduled backups, I also take manual snapshots before any major update or significant work on a VM, a habit that has saved me more than once when an update didn't go as planned.

PBS also runs verification jobs on a regular basis. This is something that often gets overlooked — a backup that can't be restored isn't really a backup. Verification ensures the stored data is intact and recoverable, not just that the job completed without an error.

The real test of any backup system isn't the setup — it's what happens when you actually need it. That moment came recently when one of my mini PCs failed completely, taking an entire PVE environment down with it. I installed Proxmox fresh on a replacement machine, connected it to PBS, and restored the VM server from the last captured backup in under a minute. The restored VM came back with its original configuration intact, including its IP address and MAC address, which meant the firewall rules and network settings required virtually no adjustment. What could have been a multi-hour rebuild turned into a minor interruption. That experience validated the entire strategy.

Off-Site and Secondary Storage

PBS on a single machine is a strong first layer, but it's still a single point of failure. To add another layer of resilience, I connected PBS to my **Synology NAS** as a secondary backup target. Once a week, PBS syncs the last ten backup sets to the Synology, giving me a secondary copy that survives even if the PBS machine itself were to fail.

The Synology adds its own layers of protection on top of that. It runs its own snapshot schedule, has replication capabilities, and maintains a copy to a dedicated physical storage drive. This creates a layered approach where each tier covers the failure scenario of the one above it, PBS covers daily recovery, the Synology covers PBS-level failures, and the physical drive covers the Synology.

Revision #1
Created 2026-05-12 01:07:12 UTC by lumxux
Updated 2026-05-12 01:09:06 UTC by lumxux