Redundancy and Backup

Redundancy

The Synology NAS system is designed with RAID (Redundant Array of Independent Disks). RAID is a data storage virtualization technology that combines multiple physical data storage components into one or more logical units for data redundancy, performance improvement, or both. Currently, my NAS is set up with two drives using RAID SHA-1, meaning these two drives mirror each other. If one disk fails or gets damaged, no data will be lost. Users won’t notice anything.
All drives are encrypted, so in the event of a break-in and theft of a hard drive, the data will remain unreadable.

Snapshots

Think of snapshots as "freezing" your files in time, allowing you to recover them later if necessary. Every snapshot creates a "restore" point, enabling file/folder recovery from a specific point in time. Each personal and shared folder is configured with snapshots. The system takes a snapshot of the folder and its contents every two hours. Snapshots are kept for 5 days, with the latest snapshot of each day retained for 30 days. You can restore a file to its state from any time in the last 5 days or to the state it was in at midnight of each day in the last 30 days.
Personal folders have an additional 3-day immutable protection, meaning the last 3 days of snapshots cannot be deleted. Even if a breach occurs, rendering files and folders locked due to ransomware, the last 3 days' snapshots cannot be deleted, providing an easy way to recover everything without paying a ransom.

Backups

All the above setups keep your files safe and allow you to restore changes. However, this is not an actual backup. Therefore, I have a daily task at night that backs up everything to an encrypted external drive, safeguarding against total device failure, viruses, ransomware, or other hacking events.
This way, your files are safe and can be recovered.

Revision #2
Created 2026-03-09 17:16:41 UTC by lumxux
Updated 2026-03-09 17:17:45 UTC by lumxux