UWM Local Networked Storage

The campus digital storage network is currently a Hewlett Packard 3PAR enterprise storage area network (SAN). This is also referred to as "Ufiles." The hardware used for storage is reviewed for replacement either every three years or based on the warranty date for current hardware.

Storage architecture:

Redundancy

- There are over 350 discs that make up the 3PAR system. Data is split between multiple discs on one "shelf," or set of 24 disks. The 3PAR system includes shelf level redundancy. This means that if a single shelf fails a second shelf takes over to keep the system running and ensure continuous availability of stored data. If both shelves go down, data will be restored from an older copy of the file.
- There may be at least 14 copies of (files) stored as backup at any one time. However, most of these copies are not "current" – they are snapshots from various times as detailed below in the "Backups" section. This includes 1-2 copies on backup to disc; a copy on the 3PAR rack; and up to twelve copies on tape.

Backups

- The current SAN includes three types of backup:
    - Type 1: VSS. This is built into the server; it allows users to do file restores in the case of accidental file deletion. This service is based on available space and the number of changes that have been made to the files, so the availability of backed up files will vary from versions going back a couple of days to a couple of months. This backup method addresses short-term file restoration for files that are frequently updated. This happens twice a day, at 7:00 a.m. and at 12:00 p.m. Central time.
    - Type 2: Veeam. These are full backups of the complete file share. These happen once per week. UITS maintains backups that go back at least 30 days. This backup method is also somewhat short term and addresses back up of entire folders or shares, in case of accidental loss due to deletion or other errors.
    - Type 3: Storage based snapshots on tape. This option is only deployed in the case of something going very wrong, such as a disaster. These backups are done on tape. A small number of daily snapshots are kept and stored temporarily. In case of major failure an entire volume could be restored to the point in time of the snapshot. Recovery time would take approximately 2-3 weeks.
- In all cases, the backups do not account for the integrity of the files – these are dutiful copies of exactly what was there at a certain point in time and does not account for or detect corruption or changes in inventory.
- Tapes are stored at the University Services and Research Building (USRB). Tape backups go back 90 days.

Remote storage

- Currently all nodes and storage that run Ufiles are in the Engineering and Mathematical Sciences (EMS) building at 3200 N. Cramer Street. Tape backups are stored in the University Services and Research (USRB) building at 115 East Reindl Way, Glendale. All sites are on-campus.
- UWM has a 30TB storage agreement with UW-Parkside, but this is not currently used for content on Ufiles (and therefore does not include UWM Libraries data).

File integrity

- There is no built-in checksum generation or fixity check currently active in the 3PAR SAN.
- Checkdisk runs semi-regularly as does defragmentation. These are block level operations that maintain the health of the system but not the files themselves (they do not detect file corruption or document file integrity.)
  - In some cases, Checkdisk and defragmentation will be run manually - this would likely happen in the event of an extremely write intense application saving to the share or if storage space runs above 80%.
- There are no audit trails for Ufiles. Keeping an audit trail for the entire system is not scalable due to the number of times files are accessed, read, and written.
  - Note: *This might be possible if all files are in a "finished" state and are not written to or accessed frequently – a consideration for future storage systems as most of the UWM Libraries archival data fit these criteria.*

System security

- Documentation of permissions and roles, access to the different storage and backup systems
  - ITAI (Information Technology Architecture and Infrastructure) provides access to the files/shares via "Group" permissions. However, file and folder level permissions are handled by CTS (Central Technology Services) or the desktop support unit for the clients that connect to the share. Direct access to the storage and backup files is limited to the ITAI team.
- Logs for read/write/deletes:
  - On normal shares these actions are not logged. This action is not sustainable at the scale of Ufiles.
- Secure storage and access:
  - We don't have anything stored in a public cloud. The physical hardware that hosts storage is only in EMS and USR Datacenters which are covered by cameras and have physical access controls in place such as Andover for entry. Only IT staff and required facilities/police have access the datacenters.