Delete means delete (90 days)

ID: EAA-001

Title: Delete means delete (90 days)

Type

Guideline

Status

Proposal

Description

When a file (or other data object) is deleted by a system or user action, no copy of the deleted data SHOULD be kept longer than 90 days.

Rationale

Many systems implement "safety net" copies of data that is deleted (aka snapshots). This copy of deleted data can provide fast, simple, and self-service data recovery from accidental deletions, malicious actions (malware / ransomware / hacker), as well as business resumption & disaster recovery scenarios. However, there is no standard default and systems implement this to different default timelimits. Examples:

- deskmail - 7 days
- gmail - 30 days
- o365 - 60 days
- physical document shredder - about 2 seconds
- Catalyst (GPFS) - 5 weeks
- Concert / Document Management system (GPFS) - 7 days
- Nebula (GPFS) - currently 1 year (only last four weeks of snapshots are directly accessible to customer)
- Nebula (Windows) - 60 days
- U Drive (GPFS) - currently 1 year (entire last year of snapshots is directly accessible to customers)
- Faculty Staff Homer home directory and web directories - currently 1 year (snapshots not easily visible to customers.)
- Student dante home directories and web directories - currently 1 year (snapshots not easily visible to customers.)
- TSM tape backup system - 45 days

Keeping deleted data available for discovery incurs a risk for the institution. Likewise, not keeping a 'safety net' copy also incurs a risk.

Keeping deleted data for long periods of time also can be a significant cost for the storage platform. Systems where the data remains until 12 months after the delete was requested are operating with up to 20% additional storage hardware costs.

Implications

What will this affect: systems for general purpose storage: Nebula GPFS filesystem, Udrive, all new general purpose storage systems (an EA exception can be requested)

Risks: Some data will be un-recoverable when asked if a copy exists after deletion.

Mitigations:

- **I**nvestigations of malware, ransom-ware, and accidental deletes need to be comprehensive in the files they review for being affected.
- System users and system designers need to consider data backup and data archive functions for their long term data storage requirements.
- Nebula has been operating with only 2 weeks of snapshots visible to customers for about a year. There have been ~ 10 requests for data > 90 days old.
- Update all service catalog entries to clarify the retention policy for deleted files, and recommend other solutions for longer term data backup and archive needs.

Domains:

Risk, Information Security

References

- https://uw.service-now.com/nav_to.do?uri=problem.do?sys_id=253a1f6b6f7b8a04bd49d5267b3ee42c

See Also

Submitted by

Date	Submitter	Role
	Brad Greer	UW-IT CTO

Reviewed by

Date	Reviewer	Role
	Brad Greer	System owner for Nebula, UDrive, Bronica GPFS
	Brian Arkills	System manager for Nebula
	David Cox	System manager for UDrive, Bronica GPFS
	Eric Horst	Infrastructure Architect
	Rupert Berk	Enterprise Architect