How to repurpose your tape library to create a cost-effective on-prem "Tape-as-Cloud" environment for Active Archive and Ransomware Protection

A QStar White Paper

QStar Technologies has been working with multiple “next generation” backup providers to provide “tape-out” functionality. Next Generation backup solutions do not typically use tape at all, preferring to use local disk-based appliances for short-term backup, paired with on-prem or public Cloud for long term backup. Tape-out is used predominantly where organizations are mandated to use tape through internal or external requirements.

What this means is that many organizations are moving away from tape for backup purposes, as it does not meet modern-day requirements for speed of retrieval and incremental backup.

At the same time, the use of tape as an active archive solution has been increasing, as cost per TB and overall data protection offered are significantly better than anything Cloud solutions can provide. Ransomware protection is almost “in-built” for tape as tape media is immutable – data cannot be overwritten, only appended. Tape is easy to copy or replicate and is easily removed, an increasing requirement is to create air-gapped content so ransomware cannot touch it.

Traditionally tape in an active archive environment was accessed through SMB, NFS or FTP, through a software or appliance gateway that accepted files and wrote any and all data to tape media for long-term preservation.

An Active Archive is defined as;

1) Active if the user that created content continues to have direct access to it, without requiring Administrator intervention and,

2) Archive if that data is protected in its own right without the need for a backup solution or third-party copy.

Today, modern gateway software (such as QStar Archive Manager) and appliances can also provide an S3 option for accessibility, opening up those increasing numbers of applications that are “Cloud-aware”, to use tape libraries as Cloud.

The two biggest concerns for Cloud users are 1) write performance – which is typically limited by expensive WAN infrastructure costs and 2) egress fees – which for large restores (such as after a ransomware attack) can be unplanned for and crippling (a 2 cent egress fee means $20,000 for 1PB).

If an organization has a tape library already, perhaps no longer being used, adding a low-cost Windows or Linux server and a QStar Archive Manager license, will very cheaply give them a very efficient Cloud option for large scale restores.

Even if a ransomware attack does start to mean content is encrypted on the tape, as tape is immutable all that will happen is that the encrypted data is written to new media. Archive Manager offers a feature called “Mount-on-Date” that winds back the clock to before the ransomware attack started to rewrite content, allowing data to be seen in the previously un-encrypted format.

Data can be written in parallel, up to the maximum tape total performance (6 x LTO6 drives writing in parallel = 960MB/sec, whereas 6 x LTO8 drives writing in parallel = 2.1GB/sec). Once the backlog of data

is written to tape, the number of drives for writes can be reduced, allowing drives for reading or hot-spares to be allocated, for the on-going write process, which is typically much less than the initial ingest.

In addition, the landing zone for data can be segregated, allowing for fast write caches and slower read-only caches to be used. Slower forms of disk-based storage (perhaps an older NAS system) can be used for reads – while a faster but small (typically under 5TB total) NVMe based write cache can be added to speed the data on its way to tape. Using disk storage as a read cache for tape allows a significant proportion of the archive to be available in sub-second timeframes.

Any version of tape can be used, standard read-write tape media is immutable, unless a tape erase of the entire media is initiated. Customers who still have LTO3 or 4 drives in libraries can create an S3 accessible store, and although slower, the principle of creating an on-prem tape-based Cloud still applies.

Tape-as-Cloud pairs very well with other public cloud options to create multi-Cloud environments, allowing system administrators to decide from where they wish to retrieve data based on capacity and expediency.

To conclude, as tape becomes less used in backup environments, we continue to see tape successfully utilized in Active Archives. Previously only accessible through file gateways, tape libraries can now also be addressed through S3 Cloud options, adding new and inexpensive options in combating the ransomware threat.