TapeTrack Implementation Planning Guide

Your corporate topography

The first step is to understand how all backup environments, either local or enterprise, can be easily implemented and used across the corporate structure, and then just as easily forgotten about, along with any knowledge or ownership. Although you may be targeting the current implementation of TapeTrack at specific backup infrastructures, be aware that it will be ideally placed to incorporate and manage any additional backup media, legacy or otherwise, to mitigate risk of data loss or compliance issues.

With this in mind it would be best practice to map out all the locations in the corporate structure that will, and could possibly be used for media management. This may include global locations, regional offices, and even broken down to individual buildings on a campus. If the initial implementation will be just part of a global enterprise, consider how best to identify the current organization and consider the implications if that were to be scaled or multiplied.

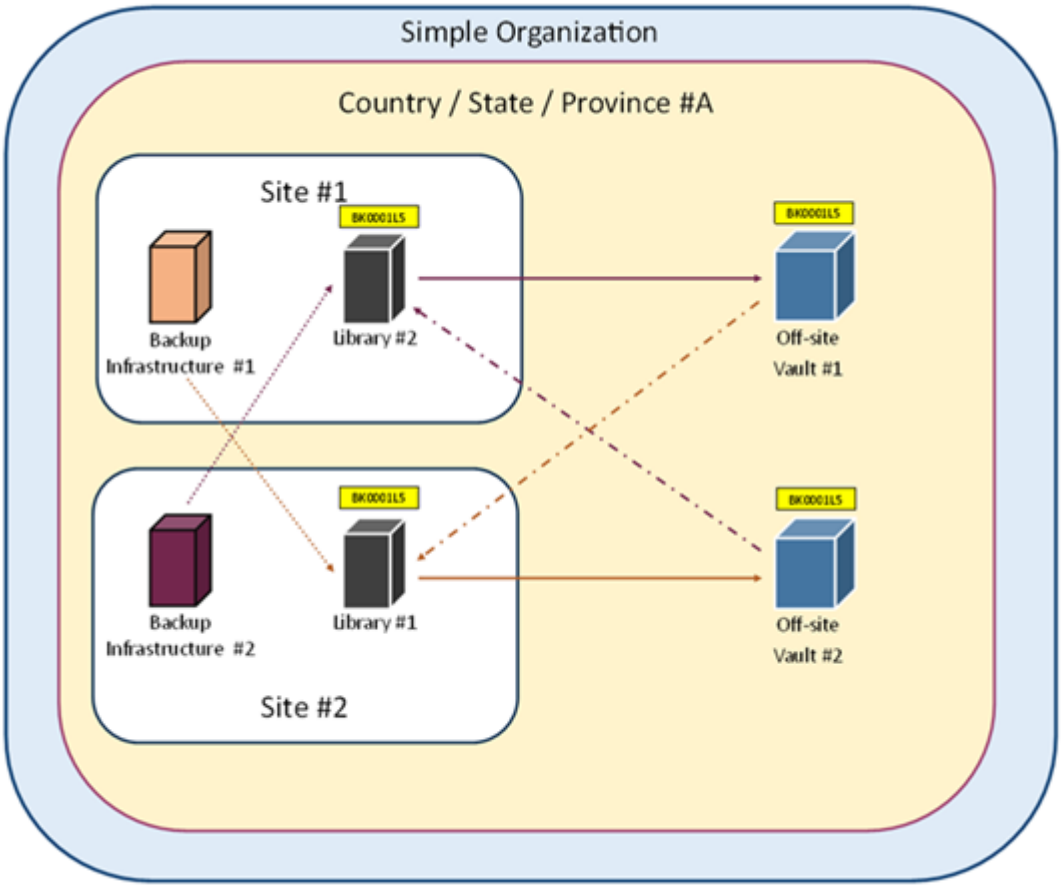
You would be advised to carefully consider individual buildings, rooms, data centers and tape libraries in addition to individual geographical locations and off-site vaults and then consider the movement of the media between these locations. This will determine how you create the Customer-ID, and therefore how you will see hierarchy in the Customer window in TapeTrack, which will be derived from every location you store or manage your media, and the relationship and movement that media has to any of those locations.

In addition please consider the movement of media if they are shared between potential Customer-IDs. It is best practice to have all the movements for any specific volumes, contained under a single Customer-ID. The good news is that due to the nature of TapeTrack, unlike larger less flexible media management products, you are able to easily customize repositories and migrate media from customer to customer should the need arise.

Be aware of common bad practice when managing media movements such as moving media between multiple libraries or sites as scratch media as the same media barcodes will be appearing on multiple reported backup infrastructures as per the example below.

Consider you have x2 different backup infrastructures, shown here as being on their own site, Site #1 and Site #2. Each site has its own backup infrastructure. For data security the backups are performed cross site. So for the Site #1, the backup data is written to media in Library #2 on Site #2, and for Site #2, the backups are written to Library #1 on Site #1.

1. Starting with the backup on Backup Infrastructure #1, the backup software picks up media barcode 'BK0001L5' and writes the backups, so that barcode will appear on the Backup Infrastructure #1, which would be the physical location Library #1, Site #2.
2. Next the media would be ejected and sent to the off-site vault, shown as Off-site Vault #2, and will appear scanned in on the off-site vault inventory.
3. To save on media it had been decided to rotate the expired media, sending it backup to Backup Infrastructure #2, Library #2 on Site #1 as scratch media, and media barcode 'BK0001L5' will now appear on that local inventory.
4. The backups are run, and the media 'BK0001L5' would be ejected and sent to the off-site vault, shown as Off-site Vault #1, and will now appear scanned on the off-site vault inventory.



Now you have the same barcode 'BK0001L5' having been written to on multiple backup inventories, and sent to multiple off-site vaults, and therefore appearing on multiple inventories within your corporate topography. Although this particular configuration can be translated into TapeTrack, is not consider best practice or recommended.

Global sites

It is very important to consider the higher level components in the structure of the organisation, even if there are not initially part of the TapeTrack implementation. Starting with the global sites, consider the hierarchy of how these will be further split into regional locations and business units with their specific media management and movement requirements.

Business units

These would be an element or segment of a company representing a specific business location or function requiring specific media management, and could be anything from a geographical location to a building, or a self-contained section of a building used as individual business premises, and requiring specific media management.

Here it would be best to consider how these need to be identified should they need to be separated or have any detailed reporting at a later stage, particularly if media is business unit specific, or if gets moved between them.

Remote sites

Depending on the movement of media, these may be considered as repositories under a Customer ID, or an individual Customer ID in their own right depending on media handling operations.

An example being that if tapes only moved to and from a regional office to a at a remote site, with a library, and a rack and/or store, these could be considered as a single repository, or repositories depending on the level of visibility and control required. This would then sit under the Customer ID, which could be the regional office. Alternatively, this may just be an off-site storage location, and not a vendor controlled vault, which could be setup as an off-site Repository ID.

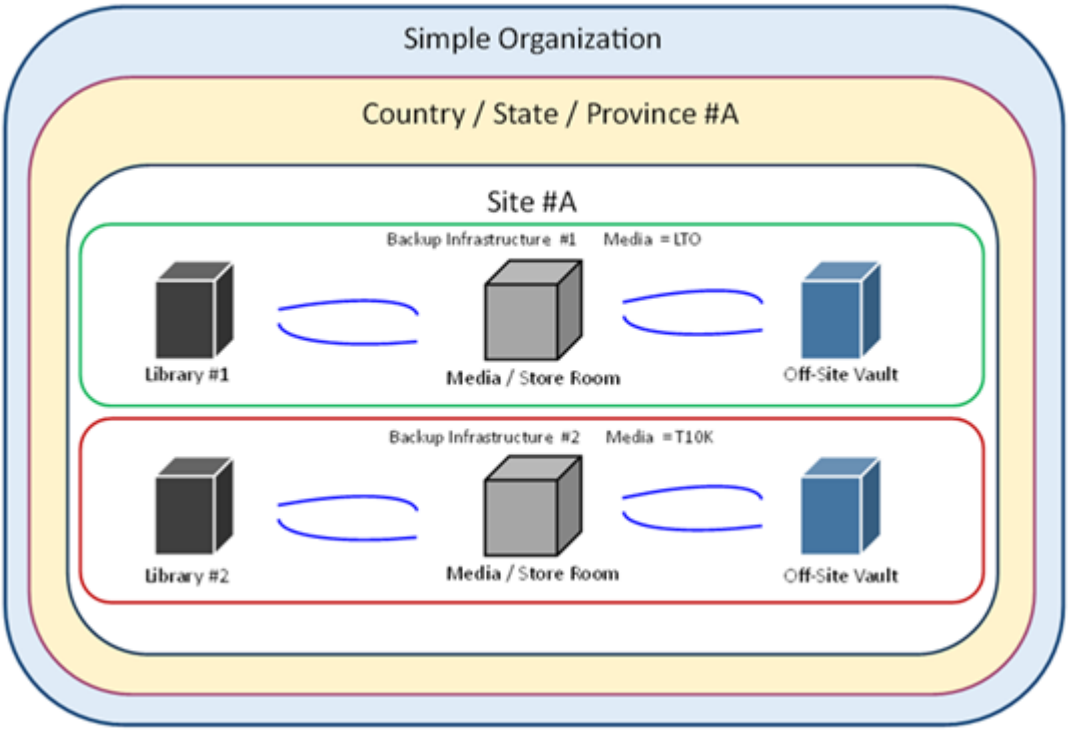
Translating Your Organisation into TapeTrack

See the examples below of how best the corporate topography and operations may be represented in TapeTrack:

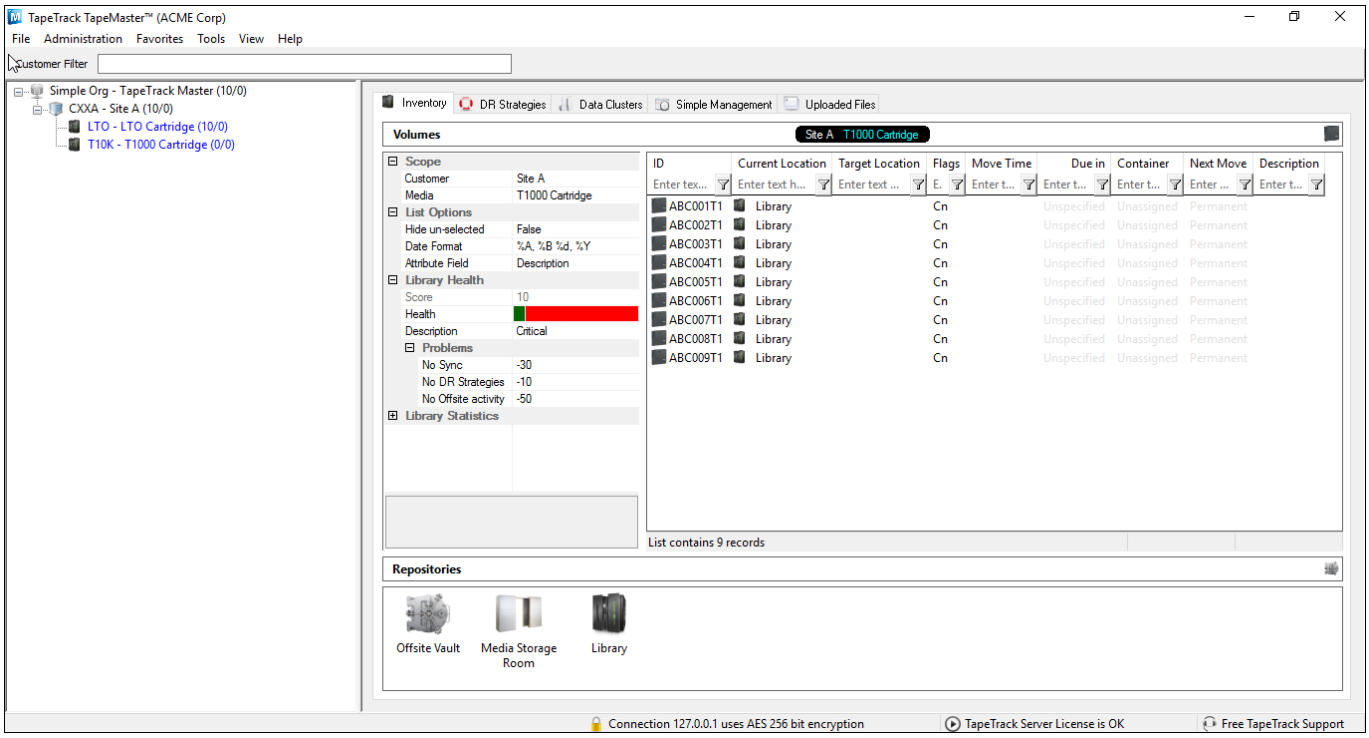
Example 1

Here an organization may have just one site, Site #A, in one country or province. At this site there may be x2 different backup infrastructures that share the same media room, for storage and media exchanges, and share the same off-site vault account.

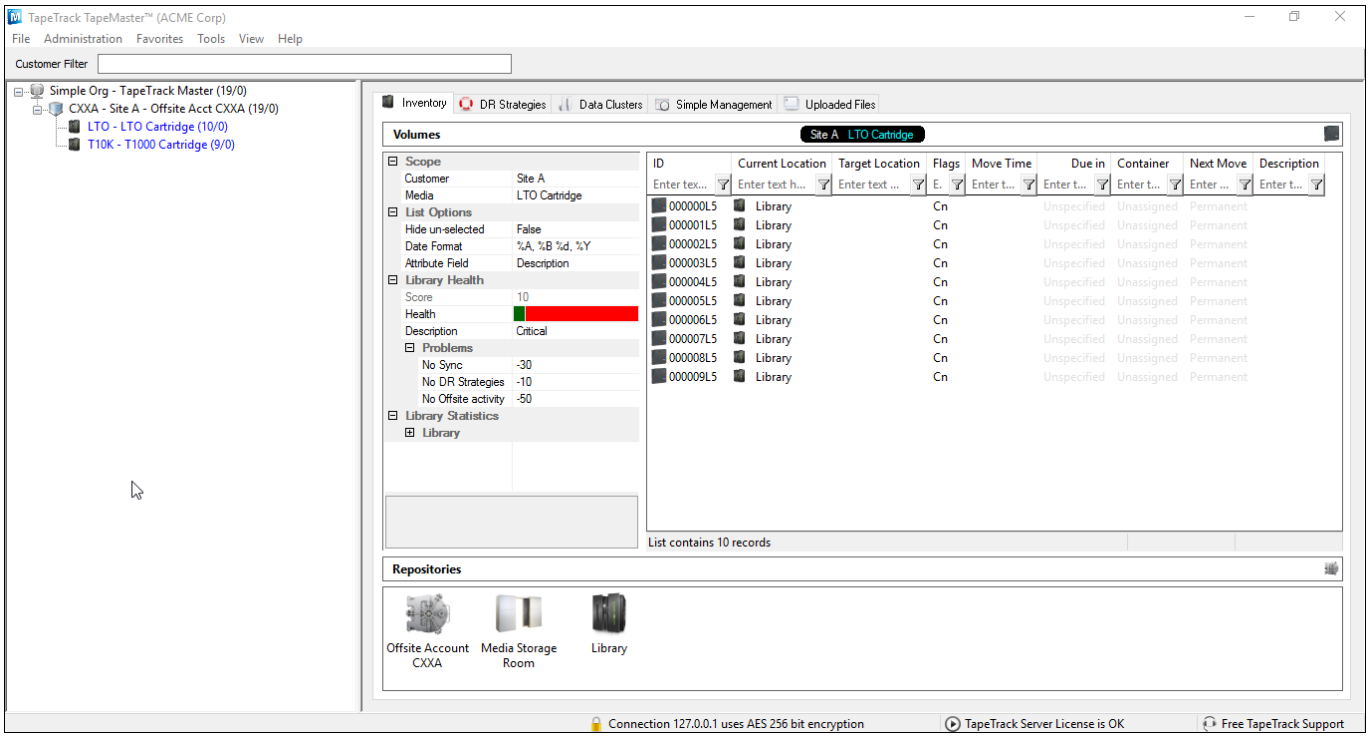
Organization Country / State / Province	Site	Backup Infrastructure	Media	Library	Racking	Store Room	Off-Site Vault
#A	#A	#1	LTO	#1		Room	Vault #1 (V001)
#A	#A	#2	T10K	#2		Room	Vault #1 (V001)



This could be translated into TapeTrack as a single Customer ID, with LTO and T10K media that would have a minimum of x3 Repository ID's per Media ID, as shown below.



Alternatively, this could be translated into TapeTrack using the off-site vault location or account number, should it be a vendor off-site vault.



However, although these x2 configurations look near identical, there are x2 important differences:

- The first configuration, which is excellent for showing the volume location in relation to the owning site, is not best suited to having the same volumes transported to any additional sites, which would be configured as Customer ID's, which may be added later.
- The second configuration, although excellent for including further sites serviced by this off-site

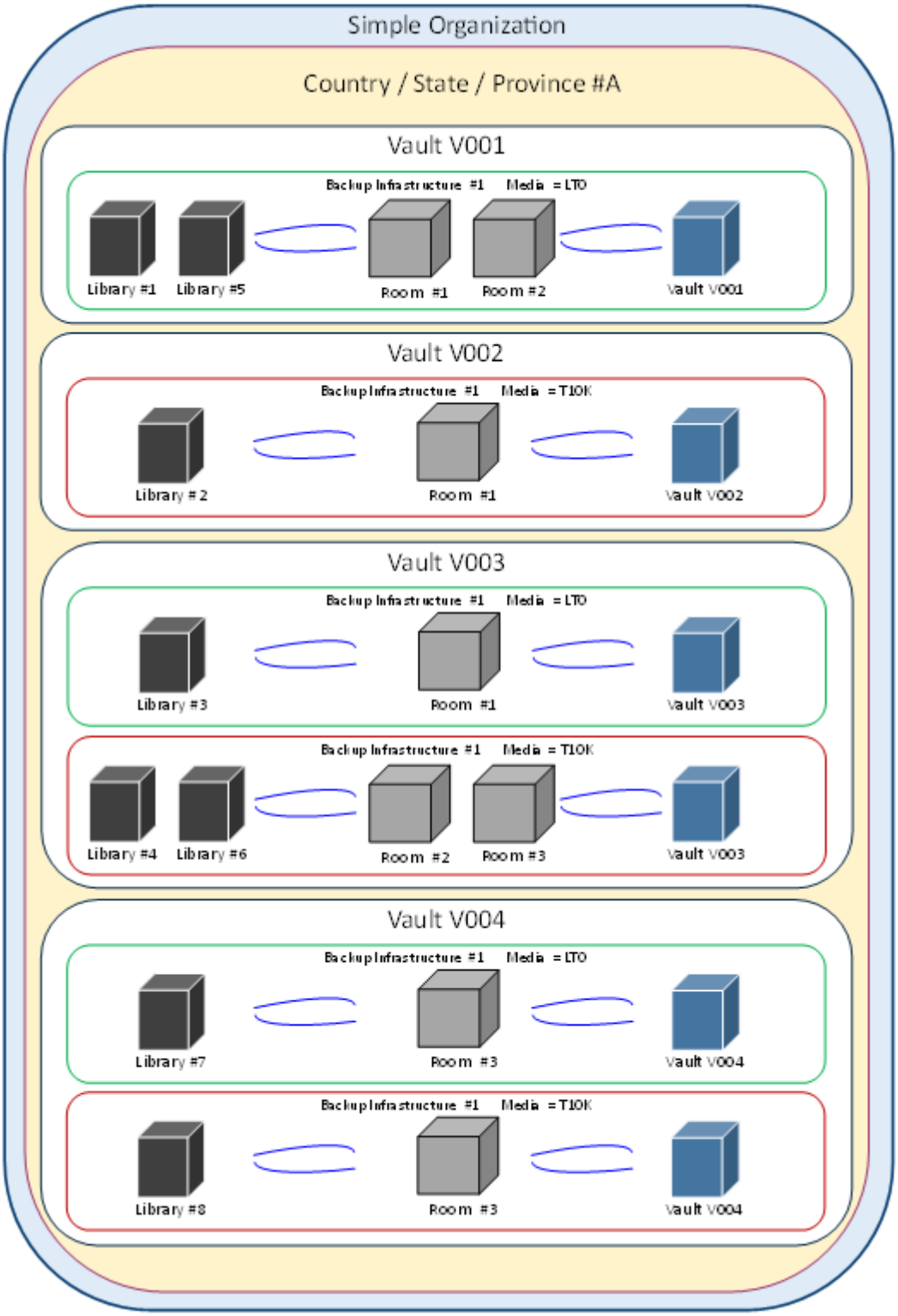
vault account, as it would be the off-site vault represented by the Customer ID, it would not be best suited to the same volumes being transported to any additional off-site vault account if required later on.

Example 2

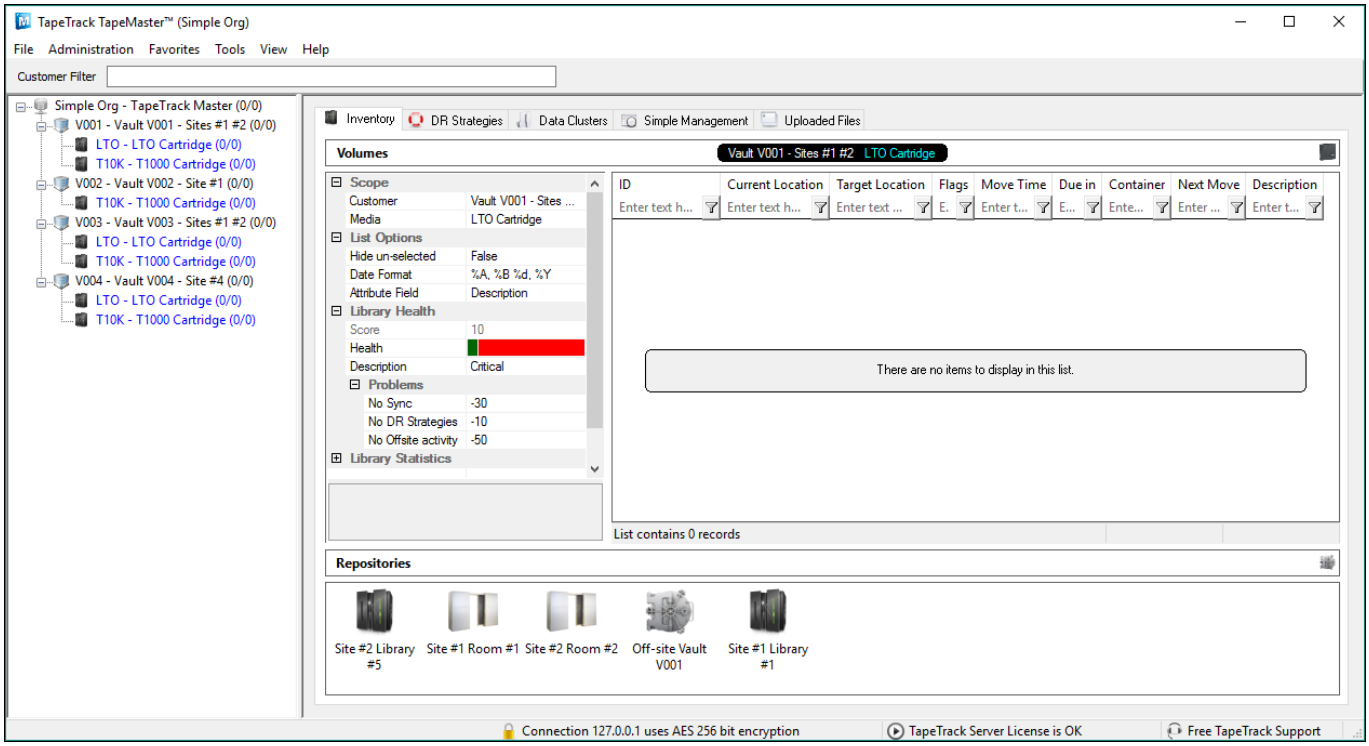
Here we have an organization with x2 sites or business units, Site #1 and Site #2, which could be in a single town, city, country or province. At each site there are x4 different backup infrastructures, where x2 allow for cross site backups. There are also local media rooms, for storage and media exchanges, but have multiple off-site vaults, but share x2 of them for the cross site media.

As media may be transported from the shared off-site vaults to either site for the cross-site backups, best practice may be to configure the off-site vaults as the Customer ID instead of the sites.

Organization Country / State / Province	Site	Backup Infrastructure	Media	Library	Racking	Store Room	Off-Site Vault
#A	#1	#1	LTO	#1		Room #1	Vault #1 (V001)
#A	#1	#2	T10K	#2		Room #1	Vault #2 (V002)
#A	#1	#3	LTO	#3		Room #1	Vault #3 (V003)
#A	#1	#4	T10K	#4		Room #1	Vault #3 (V003)
#A	#2	#1	LTO	#5		Room #2	Vault #1 (V001)
#A	#2	#2	T10K	#6		Room #2	Vault #2 (V003)
#A	#2	#5	LTO	#7		Room #3	Vault #4 (V004)
#A	#2	#6	T10K	#8		Room #3	Vault #4 (V004)



This could be translated into TapeTrack as a x4 Customer ID's representing the x4 off-site vaults, with LTO and T10K media that would still have a minimum of x3 Repository ID's per Media ID, as shown below.



This would provide the best practice for maintaining your media inventory allowing media to move between sites but having a common off-site vault.

Your current Tape Management Processes

Your current tape/media management process should include the following:

- Stock management for the purchase and storage of new media
- Scratch media management so you are aware of what tapes can be reused
- Identifying tapes to be vaulted and sent off-site
- Identify faulty tapes to identify potential data loss
- Ejection confirmation and/or Picking list confirmation
- Media exchange with any party such as an off-site vendor
- Routine media audits and certification for all media locations
- Daily media movement verification's and alerting
- Barcode management to avoid duplication in any one environment
- Regular process review or gap analysis
- Media destruction process for regulatory compliance
- Legal hold process to identify and safeguard digital media

Some of these items may be include in the media handling process for events such as the daily vault and off-siting of media. It is best practice to identify stages in the manual handling process where media may need to be identified or verified which can be captured and recorded by TapeTrack so it has an audit trail. Be aware that any locations where media may be temporarily stored or held as part of the daily movements could be considered as a repository, or a least a check box on a media handling or movement process.

For example TapeTrack can be used to audit, and in some places automate, the verification of media at each step of the media handling process, depending on the level auditing that is required. Below is a typical list of verification steps, aside from the backup software inventory and in no particular order,

required to mitigate the risk of losing any media.

- Check that the vault has run, media ejected ready to be removed from the library.
- Check for media residing in the library or device media access port after eject.
- Check of media received in a secure media room, or scanned to a rack.
- Check of media scanned into or out from a closed containers.
- Check of media scanned out for transportation to off-site vault.
- Check that media has been received at the off-site vault.
- Check of recalled media that has left the off-site vault.
- Check inventory of media in all libraries.
- Check inventory of media in all off-site vaults.
- Check inventory of media in all racks, secure rooms and store rooms.

Your current media inventory

For a complete overview and control of your media, your inventory should include, but not be limited to, the following elements, which can be imported into TapeTrack so as to enable compliant auditing and the ability for reporting and forecasting :

- Media purchased but in the store room or not called to site from the supplier.
- Scratch media availability in the store room and in the library.
- Media in libraries including details of last write date, next move date, and expiry date etc..
- Media on legal hold including details of legal hold start and finish dates, data owner, and any further legal order details.
- Media destroyed or to be destroyed with the destruction date, vendor destruction reference, authorization details etc..

Be aware of common bad practice when managing media inventories and movements such as :

- Using multiple identities for a single tape.
- Relying on handwritten labels and not using barcodes.
- Failing to identify the potential for duplicate, or triplicate barcodes when consolidating multiple or legacy backup infrastructures into a specific site or off-site vendor account.
- Moving media between multiple libraries or sites as scratch media will have the same media barcodes appearing on multiple backup infrastructures.
- Relying solely on the off-site vendors inventory as this will cause problems when media is added and used in the backup environment but never sent to the off-site vendor.
- Not keeping the history of removed or destroyed media, or not isolating details of destroyed media from the active media inventory which can result in reconciliation issues.
- Reliance of spreadsheets, as procedures may be misinterpreted, and incorrect locales may impact the management of move dates and expiry dates, with risk of incorrect media being overwritten and destroyed..
- Reliance on homegrown developed applications with risk from poor or no change control process, or reliance on a single employee.

Your backup software

Hopefully the backup software would have been installed and configured with the consideration of media management and not just backup operations. First we should note the backup software vendor,

version and platform. This way we can understand and plan around security and any reporting of file transfer locations. This will relate to how the software is queried and generates reports, and where are they located. Then we consider what commands are used or to be used to generate the required output, and try and think around any limitations or required translations.

Examples of fields you may want to include in queries, but not be limited to, are listed below :

- Volume/volid/mediaid
- Barcode
- Mediaidtype/family/type
- Poolname/pool
- Robotnumber/location
- Vaultcontainer/location
- Expiry/volretent

You may at this stage consider what barcode rules you have in place, and the impact that may have on managing the media inventory on a wider perspective. If you are in the process of implementing a new backup environment, or consolidate multiple infrastructures, be sure to make use of the full barcode if possible, including the media type suffix. This will be valueble later on in the media lifecycle. For example experience has shown media managers falling foul of reporting multiple media with the same barcode, eg. '102030', but in reality they may be '102030D', '102030L1', '102030L4', but cannot be distinguished by reporting from the backup software. TapeTrack is able to translate the barcodes during synchronisation, so they are identified correctly when reporting.

Please also consider the full lifecycle of media, from how it is added, used, stored and destroyed, and what records of the media should be kept either inside or outside of the backup software. Be aware that sometimes normal process dictates that non production,legacy or destroyed media be removed from the backup software database and not leave any history.. Or worse, the backup infrastructure is decommissioned with media information lost, but the media is still in a storeroom somewhere. With that in mind, you may wish to keep a record of the media, its history, and its destruction records and certification in TapeTrack for audit validation or compliance reasons, long after the backup infrastructure and/or media has gone.

Your backup administrators

Backup administrators may or may not be required to manage backup media as per a dedicated media management team, but it can be vitally important they have a global view of the media. This allows any business to be more efficient and proactive in handling media for data recovery, and may allow for alternative recovery media to be identified and recalled for use quicker than simply relying on expected media being available for data recovery.

When configuring access to TapeTrack it is always worth considering non media handling teams for having a read only view of appropriate Customers ID's, Media ID's, and Repository ID's.

Your operational staff

You should identify what operational staff will require access to TapeTrack, and consider what functions they need to perform.

Local tape handlers may only require access to one site, and then they may only need access to one specific set of media. However there may be staff that will perform physical audit duties across all media and all sites.

This access should be recorded and used to identify access groups that should be created in TapeTrack.

Your off-site vendor

Your off-site vendor will have an inventory and an audit trail of what media they have collected, stored and returned. Be aware that regulation may only require the off-site vendors to retain 2 to 3 years of history, so it would be best practice to maintain historical records in some form for the life of the volumes. Records should be available for synchronization with TapeTrack via a download from a web based interface at minimum. If possible it is recommended that inventory and reconciliation data be retrieved via an electronic data interface, (EDI), so the process may be automated. This is usually performed by SFTP to a vendors site, however with data security under more and more scrutiny it is worth inquiring if the have an application programming interface, (API), or can support an AS2 interface with the organisations systems.

Always remember that although the off-site vendor can supply a media inventory, this is not your organisations inventory and in some instances may only act a a guide to which media they have handled and stored. TapeTrack should be your definitive inventory.

Your tape library hardware

Aspects of tape library hardware can be often overlooked with regard to media handling and inventory audit. An inventory of the library through the backup software is normally performed upon the eject or load of tapes and is normally sufficient in most cases. However, although rare, there can be occasions where tapes may be ejected to the cap or removed entirely outside of standard operational processes. It can therefore be important to query the library at a more hardware level to retrieve an inventory of tape drives, the media access port, (CAP or MAP), and all storage slots, particularly if the library is partitioned or licensed for a specific number of slots.

Querying the library can be performed with such tools as Commvaults ArmTool or Symantec's Robtest, etc., this may also be possible via a library's web interface. The resulting inventory may then be synchronized into TapeTrack to provide a more accurate inventory.

Political Considerations

As with all all decisions that may invoke apparent change in working practice, there will be political considerations within the organisation. This may stem from replacing an existing system which requires a larger overhead, or the implications of integration changes with 3rd party application and vendors.

With any implementation, it may not just be the infrastructure and working practice, but all stakeholders that have to be considered. It would therefore be best practice to list all interested

parties, both locally and globally, and make note of any points for discussion.

Who might push back

There may be push back from persons or departments include, but not limited to, those listed below.

Managers and Financial Controllers who may :

- not understand the benefits to the media management process
- already oversee another product in another region or country
- be influenced by corporate departmental operations
- be influenced by vendor interests
- be focusing on disk or cloud based migrations

Media Movements operators that may :

- argue over the need to improve any media management system
- fear potential change in the operational procedure

Media Handlers that may :

- Fear potential change in operational procedure

Who might struggle to learn TapeTrack