Privacy Regulation Compliance with Dell PowerVault Tape Libraries

Library-managed LTO hardware encryption on Dell™ PowerVault™ tape automation libraries

Dell Product Group | Storage Engineering

March 2016

A Dell White Paper

Revisions

Date	Description
November 2007	Initial release
January 2015	Revision 2.0
September 2015	Revision 3.0
March 2016	Revision 4.0

Acknowledgements

This paper was produced by the Storage Engineering Team.

Authors:

Libby McTeer – Senior Principal Storage Engineer

Cedrick Burton – Storage Development Senior Engineer

This document is for informational purposes only and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.

Table of contents

Figures

The regulatory landscape

Laws in many states and at the federal level require protection of personally identifiable customer data, not just notification after a security breach. Due to the proliferation of personally identifiable data like credit card numbers, businesses from self-employed service providers to large enterprise companies need to take measures to be in compliance.

Federal privacy regulations such as HIPAA covering health information and the Gramm-Leach-Bliley Act covering financial data are in the news due to data breaches. Privacy laws also cover the safeguard of customer data in areas such as the cable and telecommunications industry, the US census, and the department of motor vehicles.

Library-managed encryption

Coupled with other data security practices, encryption can be a vital component of privacy compliance. Encryption can ensure that only authorized persons can access sensitive customer data even if the storage media, like a laptop, hard drive, or tape media is lost, stolen or otherwise compromised.

Encryption algorithms use encryption keys of varying lengths to obfuscate the data. Only a user with the right decryption key can view the original data once it is encrypted. The LTO-4 and later generation tape drives in Dell™ PowerVault ™ tape libraries contain hardware encryption engines using an AES-256 bit encryption algorithm. Library-managed encryption (LME) is a licensable feature on the tape libraries that provides access to the drive encryption engines.

Tape libraries are used for backup and archive of company and customer data. Dell tape libraries, library-managed encryption, and the IBM® Security Key Lifecycle Manager (IBM SKLM) software application provide a centralized library-managed encryption solution to maintain and manage the encryption keys required for compliance. A key server pair consisting of a primary and secondary (redundant) key server for high availability can manage keys for multiple PowerVault TL1000, TL2000, TL4000, and ML6000 tape libraries even in heterogeneous tape backup application environments with many sources of backup data. Tapes can be interchanged between libraries as long as access to the key server pair is maintained.

The library-managed encryption solution is designed to fit into existing customer infrastructures as well as new installations. The IBM SKLM application offers broad OS support including Microsoft® Windows®, Red Hat® Enterprise Linux®, and SUSE® Linux.

Refer to the *Library-Managed Encryption for Tape* white paper on the individual library product pages for more information on library-managed encryption.

Reference architectures

This white paper outlines two reference configurations covering the following customer sets:

- Small to medium business customers who need to protect customer data such as credit card information or medical information
- Large enterprise customers who need to protect corporate data such as intellectual property or customer data such as credit card information or other payment data

Small to medium business customers

The PowerVault TL2000 tape library is ideal for small and medium business customers. The library contains 24 storage slots and can accommodate up to two LTO drives. Drives can be added after the library is deployed to grow your backup capacity as your needs grow and IT budget is available.

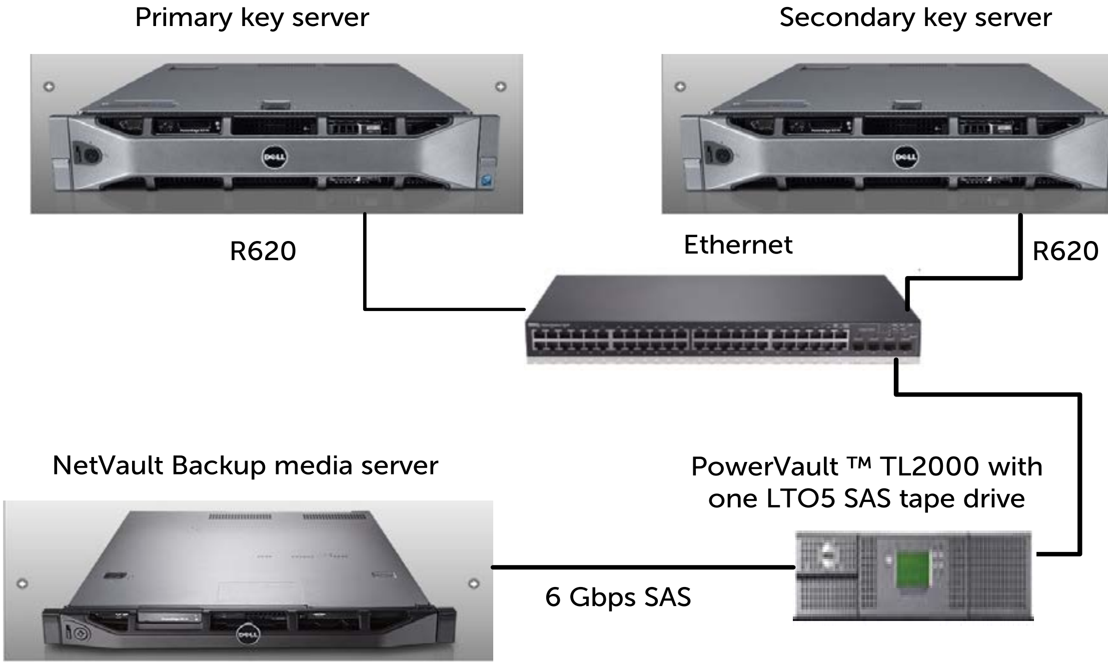
Primary key server
Secondary key server
R620
Ethernet
R620
NetVault Backup media server
PowerVault ™ TL2000 with one LTO5 SAS tape drive
6 Gbps SAS

Figure 1 Reference configuration for small to medium business customers

For this configuration, an LTO-5 SAS tape drive is used in the TL2000 tape library. The tape drive is connected to the Dell NetVault Backup media server via the Dell 6Gbps SAS HBA. Two Dell PowerEdge™ T620 servers serve as the primary and secondary key servers. You must ensure the key server performance and response time is not affected by any other applications running on the same physical server to ensure keys are available for scheduled backups.

Ensure the network on which the key servers are resident contain enough free bandwidth so communications are not interrupted. The backup job will fail if the library cannot obtain an encryption key for the drive. If the primary key server is inaccessible due to a network or server outage, the tape library will automatically fail over to the secondary key server if a secondary key server is configured in the library. The secondary key server is a copy of the primary key server so the encryption keys and configuration settings are the same between both servers.

In addition to maintaining a secondary key server for encryption key availability, customers should also observe good data backup practices. The primary key server backup required to replicate the key servers in a disaster recovery situation should be stored on unencrypted media in a safe location. The key store file is encrypted so the keys are not visible in the clear on the backup media.

Large enterprise customers

The PowerVault ML6000 tape library family offers great flexibility to large enterprise customers. The library is modular and supports physical library sizes of 5U, 14U, 23U, 32U, and 41U. The library supports up to 18 tape drives, depending on the library size. You can choose the optimal size for your current needs, then you can expand the library and drives to meet future needs.

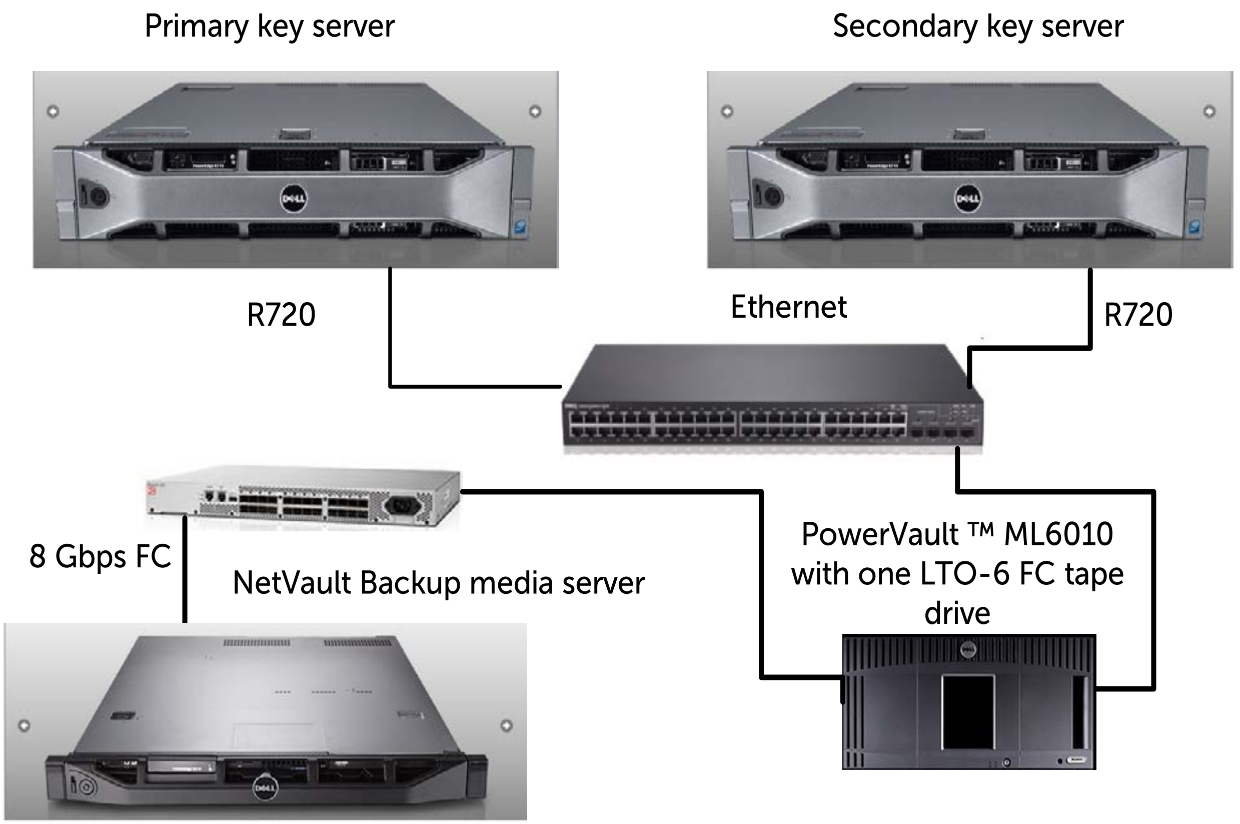
Primary key server
Secondary key server
R720
Ethernet
R720
8 Gbps FC
NetVault Backup media server
PowerVault ™ ML6010 with one LTO-6 FC tape drive

Figure 2 Reference configuration for large enterprise customers

For the large enterprise configuration, the PowerVault ML6010 tape library is the backup/archive solution. The ML6010 tape library is 5U chassis with 41 storage slots and support for one or two LTO drives. An LTO-6 Fibre Channel drive is used in the tape library in this reference architecture. The primary key server and secondary key server are hosted on PowerEdge R720 servers. The Dell NetVault Backup media server is connected to the drives via an 8Gbps Fibre Channel HBA.

Tailored privacy compliance solutions

The reference architectures in this white paper illustrate how Dell PowerVault tape libraries and library-managed encryption can provide tailored cost effective solutions for customers of all sizes requiring encryption for privacy compliance. Existing customer infrastructures of Dell tape libraries can be leveraged for this solution to keep costs low. New customer installations can be optimized for current backup needs and budgets as well.

Library managed encryption enabled PowerVault TL1000 tape libraries can be purchased at point of sale only. Library managed encryption cannot be enabled on existing TL1000 tape libraries and the feature cannot be purchased after point of sale as is the case with other PowerVault tape libraries.

Library managed encryption is only available on LTO-6 and later generation TL1000 tape libraries. Customers currently utilizing LTO-4 encrypted media will need to purchase the LTO-6 configuration due to the n-2 backwards compatible read limitation of LTO drives and media.