Privacy Regulation Compliance with Dell™ PowerVault™ Tape Libraries and the Dell Encryption Key Manager

Libby McTeer and Cedrick Burton

Dell Product Group | Storage Engineering

December 2011| Rev 1.0

Contents

Figures

The Regulatory Landscape

New laws in many states require protection of personally identifiable customer data, not just notification after a security breach. Even if a company is not located in an affected state, the laws will apply if the company maintains data from residents of that state. 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. Federal privacy laws also cover the safeguard of customer data in areas such as the cable and telecommunications industry, the US census, the department of motor vehicles, and even DVD rentals.

Library-Managed Encryption

Coupled with other data security practices, encryption can be a vital component of state and federal privacy compliance. Encryption can ensure that only authorized persons can access sensitive customer data even if the storage media e.g. 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 LTO4 and LTO5 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 which 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 Dell's Encryption Key Manager 3.0 (EKM) provide a centralized library-managed encryption solution to maintain and manage the encryption keys required for compliance. An EKM pair consisting of a primary and secondary (redundant) key server for high availability can manage keys for multiple PowerVault 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 EKM pair is maintained.

The library-managed encryption solution is designed to fit into existing customer infrastructures as well as new installations. The EKM 3.0 application offers broad OS support including Microsoft™ Windows, Red Hat Linux, and SUSE Linux.

Please refer to the *Dell™ PowerVault ™ Library-Managed Encryption for Tape* whitepaper at http://www.dell.com/downloads/global/products/pvaul/en/library_managed_encryption_for_tape.pdf for more information on library-managed encryption.

Reference Architectures

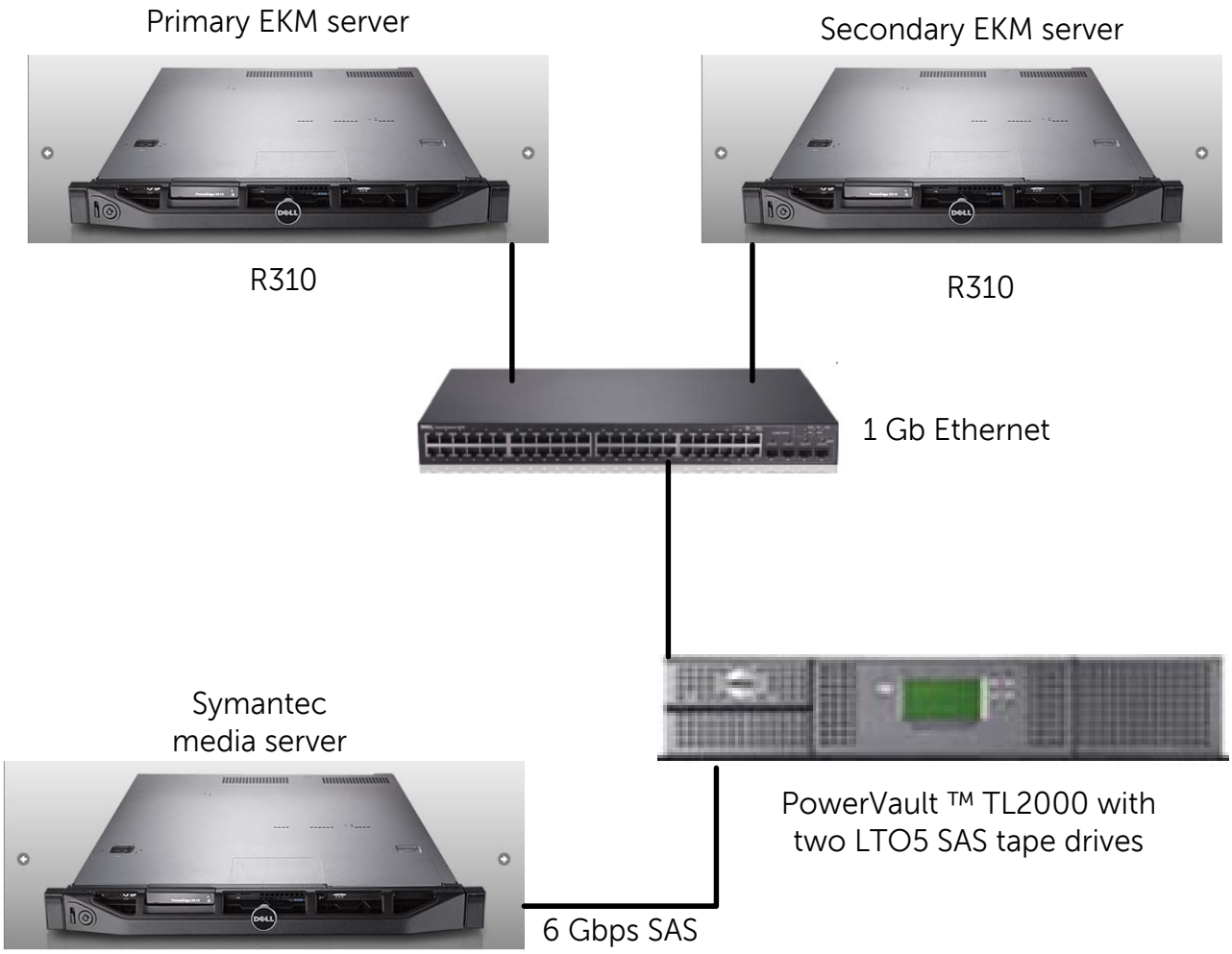
This whitepaper outlines two reference configurations covering the following customer sets:

- 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 can store up to 36 TB of data natively via LTO5 tape drives and 24 storage slots. The library can accommodate up to four LTO5 drives and drives can be added after the library is deployed. This allows customers to grow their backup capacity as their needs grow and IT budget is available.

Figure 1. Reference Configuration for Small to Medium Business Customers



For this configuration, two LTO5 SAS tape drives were used in the TL2000 tape library. The tape drives were connected to the Symantec™ media server via the 6 Gbps SAS HBA. Two PowerVault R310 servers served as the primary and secondary EKM servers. The media server is a separate server as it is recommended to install EKM 3.0 on a dedicated physical server that is not used for any other services. This will ensure that EKM 3.0's performance and response time is not affected by any other applications running on the same physical server.

The backup job will fail if the library cannot obtain an encryption key for the drive. If the primary EKM server is inaccessible due to a network or server outage, the tape library will automatically fail over to the secondary EKM server if a secondary EKM is configured in the library. The secondary EKM server is a copy of the primary EKM server so the encryption keys and configuration settings are the same between both servers.

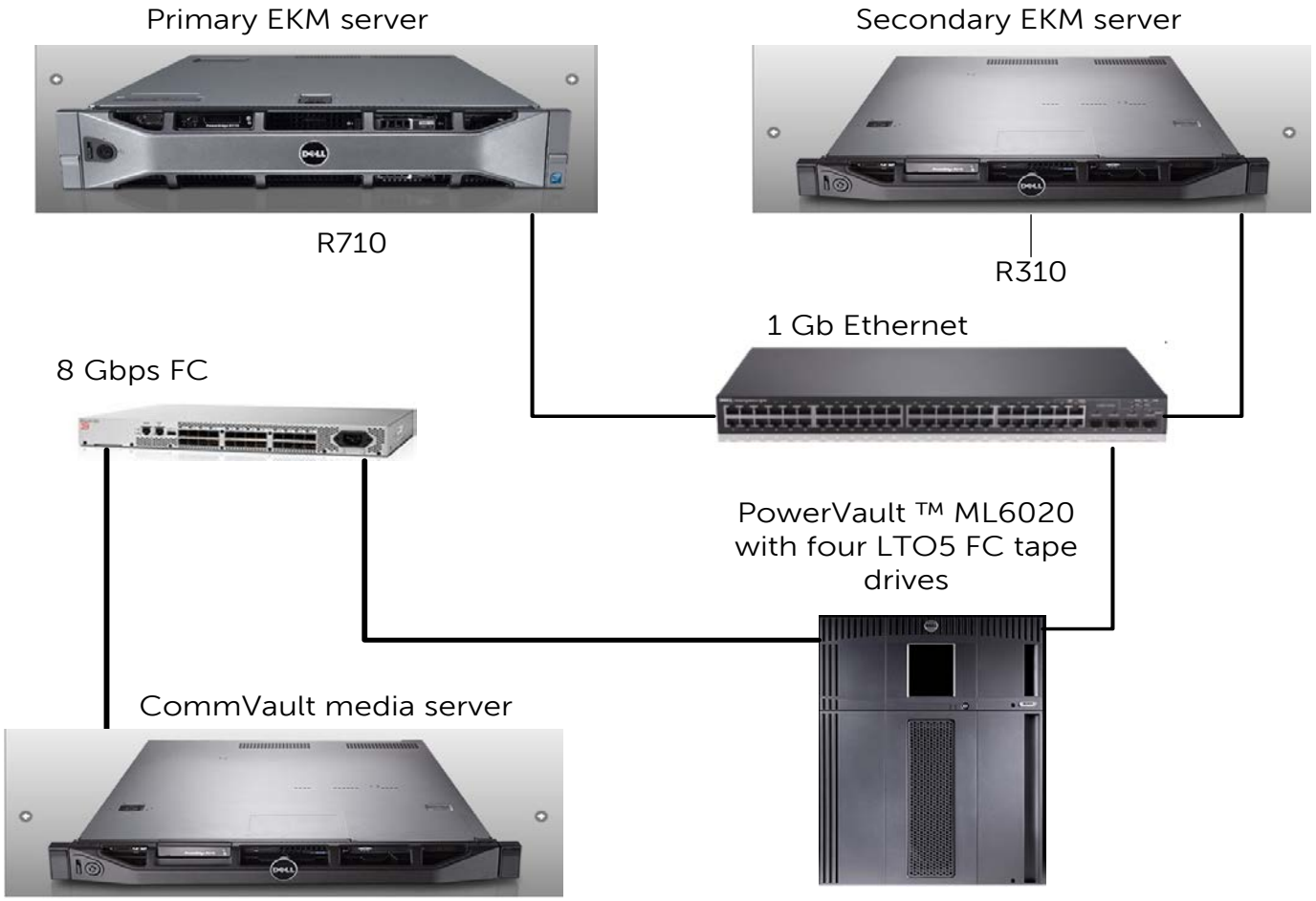
In addition to maintaining a secondary EKM server for encryption key availability, customers should also observe good data backup practices. The key store and other files required to replicate the EKM servers in a disaster recovery situation should be stored on unencrypted media in a safe location. The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

EKM 3.0 is not network traffic intensive so the onboard 1 Gb Ethernet LOMs in the R310 servers are acceptable for the EKM connection. Customers must ensure the network on which the EKM servers are resident contain enough free bandwidth so that EKM communications are not interrupted. If the EKM cannot provide the encryption key before the drive timeout, the backup job will fail.

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 between 2 and 18 tape drives, depending on the library size. Customers can choose the optimal size for their current needs and know the library and drives will expand to meet future needs.

Figure 2. Reference Configuration for Large Enterprise Customers



For the large enterprise configuration, the PowerVault ML6020 tape library was chosen for the backup/archive solution. The ML6020 tape library is 14U and can store up to 199.5 TB natively via LTO5 tape drives and 133 storage slots. Four LTO5 Fibre Channel drives were used in the tape library. The primary EKM is hosted on a PowerEdge™ R710 server and the secondary EKM is hosted on a PowerEdge R310 server. The CommVault media server is connected to the LTO5 Fibre Channel drives via a Brocade 815 Fibre Channel HBA. As in the previous configuration, the onboard 1 Gb Ethernet LOMs on the EKM servers are acceptable for EKM communications. The same concern about overall network bandwidth applies here as well.

Tailored Privacy Compliance Solutions

The reference architectures in this whitepaper illustrate how Dell PowerVault tape library and the Dell Encryption Key Manager 3.0 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.