Advanced Encryption and VTL Features Give Organizations New Impetus to Use the Dell DR Series as their "One Stop Shop" Backup Target

To simplify their backup environments, organizations desire backup solutions that essentially function as "one-stop shops" to satisfy their multiple backup requirements. To succeed in this role, they should provide needed software, offer NAS and virtual tape library (VTL) interfaces, scale to high capacities and deliver advanced encryption capabilities to secure backup data. By Dell introducing advanced encryption and VTL options into its latest DR 3.2 OS software release for its DR Series, it delivers this "*one-stop shop*" experience that organizations want to implement in their backup infrastructure.

The More Backup Changes, the More It Stays the Same

Deduplicating backup appliances have replaced tape as a backup target in many organizations. By accelerating backups and restores, increasing backup success rates and making disk-based backup economical, these appliances have fundamentally transformed backup.

Yet their introduction does not always change the underlying backup processes. Backup jobs may still occur daily; are configured as differential, incremental or full; and, are managed centrally. The only real change is using disk in lieu of tape as a target.

Even once in place, many organizations still move backup data to tape for long term data retention and/or offsite disaster

recovery. Further, organizations in the finance, government and healthcare sectors typically encrypt data such as SEC Rule 17a-4 specifies or the 2003 HIPAA Security Rules and more recent 2009 HITECH Act strongly encourage.

Continued Relevance of Encryption and VTLs in Enterprises

This continued widespread use of tape as a final resting place for backup data leads organizations to keep current backup processes in place. While they want to use deduplicating backup appliances, they simply want to swap out existing tape libraries for these solutions. This has given rise to the need for deduplicating backup appliances to emulate physical tape libraries as virtual tape libraries (VTLs).

A VTL requires minimal to no changes to existing backup-to-tape processes nor does it require many changes to how the backup data is managed after backup. The backup software now backs up data to the VTL's virtual tape drives where the data is stored on virtual tape cartridges. Storing data this way facilitates its movement from virtual to real or physical tape cartridges and enables the backup software to track its location regardless of where it resides.

VTLs also accelerate backups. They give organizations more flexibility to keep data on existing SANs which negates the need to send data over corporate LANs where it has to contend with other network traffic. SAN protocols also better support the movement of larger block sizes of data which are used during backup.

Finally, VTLs free backup from the constraints of physical tape libraries. Creating new tape drives and tape cartridges on a VTL may be done with the click of a button. In this way organizations may quickly create multiple new backup targets to facilitate scheduling multiple, concurrent backup jobs.

Encrypting backup data is also of greater concern to organizations as data breaches occur both inside and outside

of corporate firewalls. This behooves organizations to encrypt backup data in the most secure manner regardless if the data resides on disk or tape.

Advanced Encryption and VTL Functionality Central to Dell DR Series 3.2 OS Release

Advanced encryption capabilities and VTL functionality are two new features central to Dell's 3.2 operating system (OS) release for its DR Series of deduplicating backup appliances. The 3.2 OS release provides organizations a key advantage over competitive solutions as Dell makes all of its software features available without requiring additional licensing fees. This applies to both new DR Series appliances as well as existing Dell DR Series appliances which may be upgraded to this release to gain full access to these features at no extra cost.

The 3.2 OS release's advanced encryption capabilities use the FIPS 140-2 compliant 256-bit Advanced Encryption Standard (AES) standard to encrypt data. By encrypting data that conforms to this standard ensures that it is acceptable to federal agencies in both Canada and the United States. This also means that organizations who are in these countries and need to comply with their regulations are typically, by extension, in compliance when they use the DR Series to encrypt their backup data.

The 3.2 OS release implements this advanced encryption capability by encrypting data after its inline deduplication of the backup data is complete. In this way, each DR Series appliance running the 3.2 OS release deduplicates backup data as it is ingested to achieve the highest possible deduplication ratio as encrypting data prior to deduplication negatively impacts deduplication's effectiveness. Encrypting the data after it is deduplicated also reduces the amount of overhead associated with encryption since there is less data to encrypt while keeping the overhead associated with the

encryption on the DR Series appliance. In cases where existing DR4100s are upgraded to the 3.2 OS release, encryption may be done post-process on those data volumes that have previously been stored unencrypted in the DR4100's storage repository.

The VTL functionality that is part of the 3.2 OS release includes options to present a VTL interface on either corporate LANs or SANs. If connected to a corporate LAN, the NDMP protocol is used to send data to the DR Series while, if it is connected to a corporate SAN, the iSCSI protocol is used.

Every DR Series appliance running the 3.2 OS release may be configured to present up to four (4) containers that each operate as separate VTLs. Each of these individual VTL containers may emulate one (1) StorageTek STK L700 tape library or an OEM version of the STK L700; up to ten (10) IBM ULT3580-TD4 tape drives; and, up to 10,000 tape cartridges that may each range in size from 10GB to 800GB.

As each individual VTL container on the DR Series appears as an STK L700 library to backup software, the backup software manages the VTL in the same way it does a physical tape library: it copies the data residing on virtual tape cartridges to physical tape cartridges and back again, if necessary. With this functionality available on leading enterprise backup software products such as Dell NetVault, CommVault Simpana, EMC Networker, IBM TSM, Microsoft Data Protection Manager (iSCSI only), Symantec Backup Exec and Symantec NetBackup, each of these can recognize and manage the Dell DR Series VTL as a physical STK L700 tape library, carry forward existing tape copy processes, implement new ones if required, and manage where copies of tape cartridges—physical or virtual—reside.

Dell's 3.2 OS Release Gives Organizations New Impetus to Make Dell DR Series Their "One Stop Shop" Backup Target

All size organizations want to consolidate and simplify their backup environments and using a common deduplicating backup appliance platform is one excellent way to do so. Dell’s 3.2 OS release for its DR Series gives organizations new impetus to start down that path. The introduction of advanced encryption and VTL features along with the introduction of 6TB HDDs on expansion shelves for the DR6000 and the availability of Rapid NFS/Rapid CIFS protocol accelerators for the DR4100 provide the additional motivation that organizations need to non-disruptively introduce and use the DR Series in this broader role to improve their backup environments even as they keep existing backup processes in place.