BEST PRACTICES GUIDE FOR DATA PROTECTION WITH CONTROLLERS RUNNING FCP

Nick Wilhelm-Olsen, Brett Cooper | TR-3202

TECHNICAL REPORT

NetApp, a pioneer and industry leader in data storage technology, helps organizations understand and meet complex technical challenges with advanced storage solutions and global data management strategies.

Table of Contents

NetApp Inc.

1. Introduction

Enterprise corporations around the globe are facing a wide variety of challenges. Challenges from competitors, economic conditions, resource limitations, and other factors make it difficult for a corporation to thrive and grow. For these companies to succeed, they rely on their enterprise storage vendors to provide constant data availability and absolute protection from data loss and corruption.

NetApp has always been a leader in providing the highest level of availability and protection to corporations, as well as educating customers on the best methods for protecting data in their unique environments.

NetApp is committed to providing fast, simple, highly available, and flexible solutions. In keeping with this tradition, NetApp has now added support for the Fibre Channel protocol (FCP) to its core line of controllers. Now, SAN and NAS technologies are available together on the same physical device with the same level of performance, availability, and simplicity that NetApp has provided for over a decade.

The purpose of this paper is to educate the reader on the best methods for protecting controllers utilizing the Fibre Channel protocol. The paper opens with a brief discussion of available data protection technology from NetApp. Next, it outlines potential configurations for data protection of FCP-only controllers as well as controllers configured for both FCP and NAS data.

2. Data Protection Overview

In order to discuss models for data protection, it is necessary to first describe the technologies used in these models. This section briefly describes all of these elements. Further explanation as well as command syntax and examples can be found in the *Data ONTAP™ Data Protection Guide*, available online at the NetApp™ NOW™ Web site—registration is required.

2.1. Snapshot™ Technology

The NetApp Write Anywhere File Layout, or WAFL™, supports Snapshots, a unique feature that allows administrators to maintain multiple read-only versions online per controller volume. Snapshots, an included component of Data ONTAP software, allow users to recover accidentally damaged or deleted data by utilizing a version of the data from within a Snapshot directory. Snapshots are described in detail in the paper entitled *SnapMirror® and SnapRestore®: Advances in Snapshot Technology* at http://www.netapp.com/tech_library/3043.html.

2.2. SnapRestore

SnapRestore software leverages the Snapshot feature of Data ONTAP software by restoring a file system to an earlier preserved state. It can be used to recover from a corrupted database or application, or damaged file system. The system administrator can restore a single logical unit number (LUN) or the entire volume containing the LUN to any existing Snapshot. Restored LUNs are available for full production use without rebooting the controller, having returned to the precise state that existed when the selected Snapshot was created. Restoration will take less than a minute regardless of the size of the LUN or volume being restored.

2.3. SnapMirror

SnapMirror provides a fast, flexible enterprise solution for asynchronous mirroring or replicating data from one controller to another over local or wide area networks. SnapMirror transfers Snapshots from specific points in time to other controllers or NearStore™ appliances. These replication targets can be in the same data center connected via a LAN (local area network) or distributed across the globe connected via MAN (metropolitan area network) or WAN (wide area network) networks. Since it operates at the changed block level instead of transferring entire files or file systems, it greatly reduces bandwidth and time requirements for replication.

2.4. SnapVault™

SnapVault software builds on the asynchronous, block-level incremental transfer technology of SnapMirror by providing archival technology. This allows data to be backed up via Snapshots on a controllers and transferred on a scheduled basis to a destination controller or NearStore appliance. These Snapshots can be retained on the destination for many weeks or even months, allowing recovery operations to occur nearly instantaneously from this destination system to the original controller.

2.5. SnapDrive™

SnapDrive software offers a rich set of capabilities to virtualize and enhance storage management for Microsoft® Windows® environments. It is tightly integrated with Microsoft NTFS, providing a layer of abstraction between application data and physical storage associated with that data. It facilitates creation and management of virtual devices on the controller, and allows the creation and management of Snapshots either from the Microsoft MMC or via a command line interface.

Storage managed by SnapDrive logically appears to the Windows host as locally attached storage. In reality, the capacity comes from a centrally managed pool of networked storage equipped with enhanced attributes. SnapDrive runs on a Windows 2000 host and complements native NTFS volume management with virtualization capabilities. It allows administrators to easily create virtual disks from pools of storage that can be distributed among several storage appliances. SnapDrive is included at no additional charge with the NetApp® Windows Host Attach Kit 1.0.

2.6. Native Tape Backup and Recovery

NetApp controllers support backup and recovery from local, Fibre Channel, and Gigabit Ethernet SAN-attached tape devices. Support for most existing tape drives is included as well as a method for tape vendors to dynamically add support for new devices. In addition, the RMT protocol is fully supported, allowing backup and recovery to any capable system. Backup images are written using a derivative of the BSD dump stream format, allowing full file system backups as well as nine levels of differential backups.

2.7. Network Data Management Protocol (NDMP)

The Network Data Management Protocol, or NDMP, is an open standard for centralized control of enterprise-wide data management. The NDMP architecture allows backup application vendors to control native backup and recovery facilities in NetApp controllers and other file servers by providing a common interface between backup applications and file servers.

NDMP separates the control and data flow of a backup or recovery operation into separate conversations. This allows for greater flexibility in configuring the environment used to protect the data on NetApp controllers. Since the conversations are separate, they can originate from different locations, as well as be directed to different locations, allowing greater flexibility in designing NDMP-based topologies. Available NDMP topologies are discussed in detail in the Data Protection Solutions Overview at http://www.netapp.com/tech_library/3131.html.

2.8. Host-Based Backup and Recovery

Host-based backup and recovery is the most common method for protecting data stored within Fibre Channel LUNs. Backup and recovery operations are performed by systems that have access to the LUN, rather than the controller where the LUN resides. Since the host or application server can understand and interpret the data within the LUN, this will be the recommended method for data protection for most applications as it allows more precise backup and recovery operations.

3. Configuration Models

Presented below are some of the possible models for data protection with FCP-enabled controllers. This is not intended to be a complete list, but rather a collection of some of the best models for most environments. Using the guidelines and recommendations presented in this document as well as other documents from NetApp, it should be possible to adapt these configurations to each unique environment.

Initially host-based data protection models are examined, specific to the type of data accessed via FCP. Next is a discussion of controller-based protection models and situations where they should be implemented. Finally, models using a NearStore appliance as a staging area for backups are presented for best performance.

3.1. Simple Host-Based Backup and Recovery Models

Determining the best model of host-based backup and recovery is entirely dependent on the class of applications in use and how they are configured. Applications are considered below by the method used to organize data, such as UFS, NTFS, Snapshot image-capable file systems such as Symantec File System (VxFS) or raw partitions. Logical volume managers such as Symantec Volume Manager (VxVM) will also be discussed.

The diagram below represents a network and storage design for the servers and devices used in these models. For simplicity, this diagram does not reflect the Ethernet management network that must exist for managing NetApp controllers.

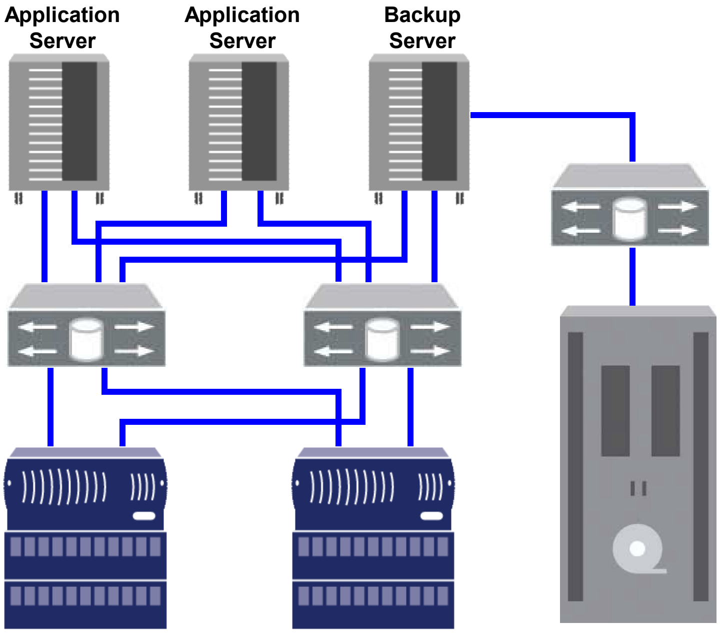

Figure 1) Host-Based SAN Backup/Recovery Diagram

The above diagram depicts a SAN with two application servers, two controllers, and a backup server all redundantly attached to two fabric switches, avoiding single points of failure. The backup server is also attached to a separate SAN for tape backup. For simplicity, this SAN is not depicted with redundant connections although that is recommended for a highly available backup environment. Zoning can be configured to support attaching tape devices to the SAN if using a third switch is not desired.

Tape libraries and drives can either be SCSI- and/or ACSLS™ (Automated Cartridge System Library Software)-attached to the backup server or attached through a Fibre Channel SAN as depicted above.

3.1.1. Non-Snapshot Capable File Systems

Applications that are implemented on top of ble file systems that are not capable of Snapshots, such as UFS or NTFS, represent the simplest scenario from a backup and recovery perspective. When backing up these applications, they must first be quiesced, or taken offline, to avoid open files or files changing during the backup operation. Then, file system caches must first be committed before the backup operation commences. The application remains quiesced or offline until the backup is completed, at which point normal application operation can resume.

This can result in a significant period of unavailability for the application. Some applications have a built-in “hot backup” mode, allowing a backup to occur while the application operates at a reduced efficiency and often limited capabilities. This type of mode is typical in messaging and database applications such as Microsoft Exchange and Oracle®. It will result in higher overall application availability than without using hot backup mode. However, it can still potentially result in a long interval of reduced efficiency and limited performance. Further instructions for backup and recovery of databases utilizing NetApp SAN configurations can be found in the NetApp Technical Library.

One final alternative is to use an open file manager from a backup software vendor. These applications are designed to handle backup operations on files that are still locked by an application. They work well for simple applications such as home directories and shared documents. However, they should be avoided with complex applications, such as messaging applications or databases.

3.1.2. File Systems Capable of Snapshots

The previous section discusses some methods to avoid potentially long periods of application unavailability, but that may result in reduced performance and function during backup. Utilizing a file system such as Symantec VxFS that allows the creation of Snapshots of the active file system can help decrease application downtime. By backing up a Snapshot of the file system, the original file system can remain online. This minimizes any application downtime or periods of reduced functionality required during backup operations.

File systems capable of Snapshots are frequently used for applications that do not provide a hot backup mode. These applications must normally be taken offline for the duration of the backup operation, usually referred to as a cold backup. Cold backups are also preferable in database environments where rollforward recovery is not possible or enabled. With file systems capable of Snapshots, the application or database is only taken offline for the duration of Snapshot creation instead of the entire backup operation.

The Snapshot file system can also be mounted and used directly should the original file system become damaged or corrupt. The Snapshot of the file system will take little time to create and restore. The Snapshot occupies little additional disk space, since it is only a copy of the changed blocks from a point in time of the active file system. For most file systems, a volume or LUN containing approximately 15% of the original file system size will be adequate to hold the Snapshot and any Snapshot iterations.

When a Snapshot is backed up, the data that has not changed is read from the original file system. Any changed data is read directly from the Snapshot. This may result in a small degradation of application responsiveness since both blocks from the active file system and changed blocks in the Snapshot are read during backup.

3.1.3. Raw Partitions

Some applications have the ability to work directly with raw device partitions, allowing significant performance benefits. In order to back up this application data, however, it is necessary to use specialized modules from a backup software vendor tailored for each application. Without these modules, there is no means of knowing if the data is in a consistent state for backup.

When backing up raw partitions, it is usually necessary to place the application in hot backup mode to ensure that the data is consistent. As there is no file system exposed outside of the application, there is no method of performing Snapshots from the host system. Thus, the application must remain in hot backup mode for the duration of the backup operation. Further instructions for backup and recovery of databases utilizing NetApp SAN configurations can be found in the NetApp Technical Library.

3.1.4. LUN Snapshots

Data ONTAP provides another method to increase application availability during backup operations. It is possible to use the WAFL Snapshot technology to provide Snapshots for the LUN, regardless of whether or not the file system on the LUN provides Snapshots or the LUN is used as a raw device. First, the application is quiesced or placed in hot backup mode, then file system caches are committed. Next, a Snapshot is created on the controller volume containing the LUN. Normal application operation can now resume. A new LUN is created that points to the LUN within the created Snapshot. This LUN can now be backed up at any convenient time. When backup is complete, the LUN and Snapshot are destroyed.

Since WAFL Snapshots occur almost instantaneously, this solution offers a significant benefit in availability, as the application is only quiesced, in hot backup mode, or, during Snapshot creation, in cold backup mode. In addition, LUN Snapshots can be combined with SnapMirror or SnapVault software to transfer these Snapshots to an alternate controllers to completely offload from the source controller any overhead from data protection on the LUN.

3.1.5. Logical Volume Managers

In the previous four configurations, file systems and partitions were restricted to one LUN and, therefore, one controller. With a logical volume manager such as Symantec VxVM, it is possible to create file systems and partitions that span many LUNs and even controllers. This can be done to increase performance by striping multiple LUNs together to appear as one larger LUN. It can also be done to increase availability by mirroring LUNs. Both operations can even be done simultaneously to mirror concatenated or striped LUNs for performance and availability.

Mirroring can also be used for performing backups. Mirroring increases application availability and can be used to offload backup overhead from application and file servers. When using a logical volume manager for backup and recovery, it is suggested that a mirror be initiated when a volume is created. This will reduce the time required to mirror the data across volumes before backup operations commence. The difference in performance can be significant with large databases. For example, a 500GB database residing on a volume can take upwards of 15 minutes to mirror to another volume.

Using mirroring, the application is quiesced or placed in hot backup mode, then file system caches are committed. The mirror relationship is broken and normal application operation resumes. At this point, the split mirror can be backed up with a host-based backup application at a convenient time. Once the backup is completed, the mirror can be resynchronized to capture any changes to the data that may have occurred while the mirror relationship was broken. This process is known as split mirror resynchronization. It will degrade the performance of the primary volume being mirrored until resynchronization is completed. As a result, these activities should be scripted and scheduled during periods of low activity, such as late in the evening or on the weekend.

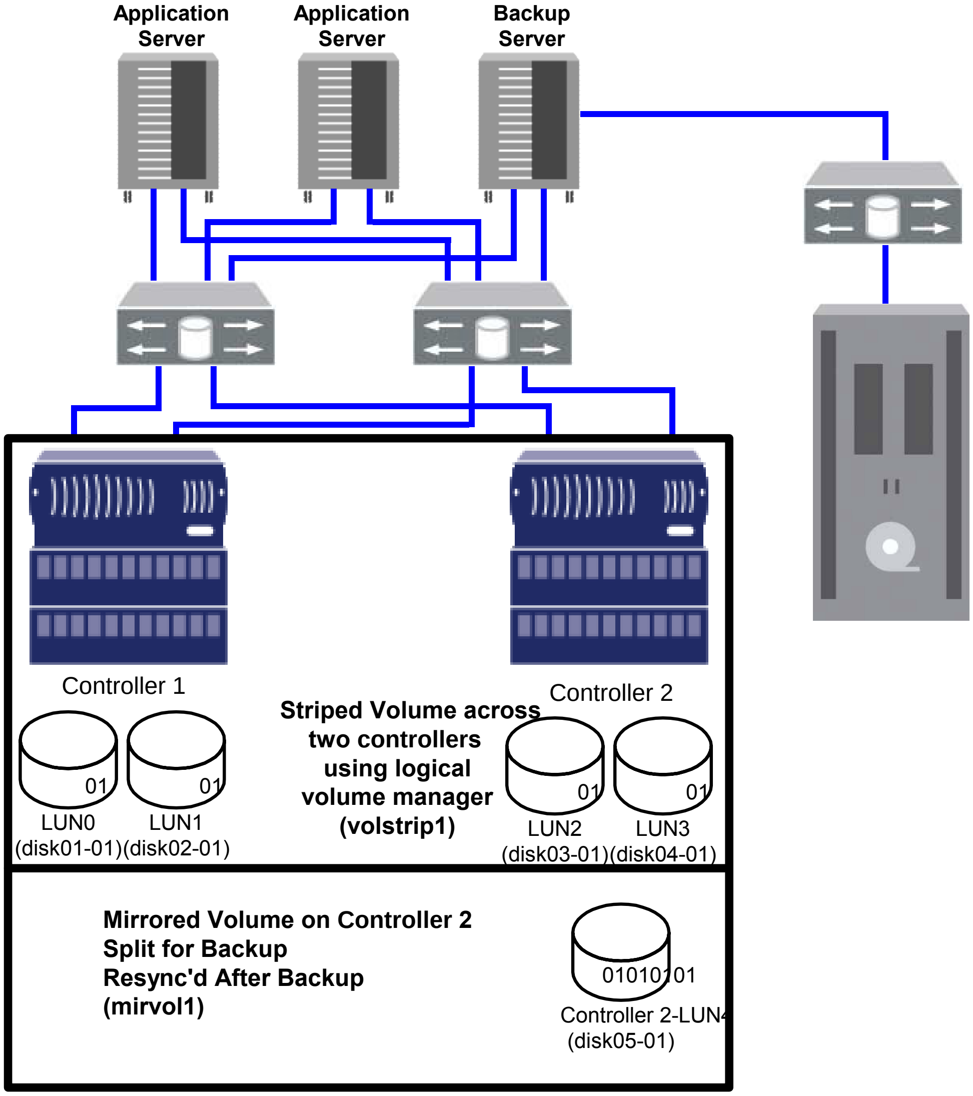

Figure 2) Backup Using a Logical Volume Manager and a Split Mirror

3.2. Simple Controller-Based Backup and Recovery Models

In certain situations where file systems or raw partitions consist of a single LUN, it will be desirable to perform backup and recovery operations directly on the controller instead of through the SAN. Using controller-based backup and recovery offloads the majority of backup overhead from the host system as well as the application SAN. In addition, full backup and recovery operations are significantly faster when performed native to the controller instead of through the application SAN. Controller-based data protection should not be considered in situations where file systems span multiple LUNs via Symantec Volume Manager or a similar product. In addition, they should not be considered when selective restoration of files within the LUN is a requirement. Controller-based data protection models always operate at the LUN level. The controller has no method of interpreting the data within the LUN itself. Incremental operations will properly transfer all changed blocks within the LUN.

The diagram below represents a network and storage diagram for the servers and devices used in the controller -based data protection models below. For simplicity, this diagram does not reflect the Ethernet management network that must exist for managing NetApp controllers.

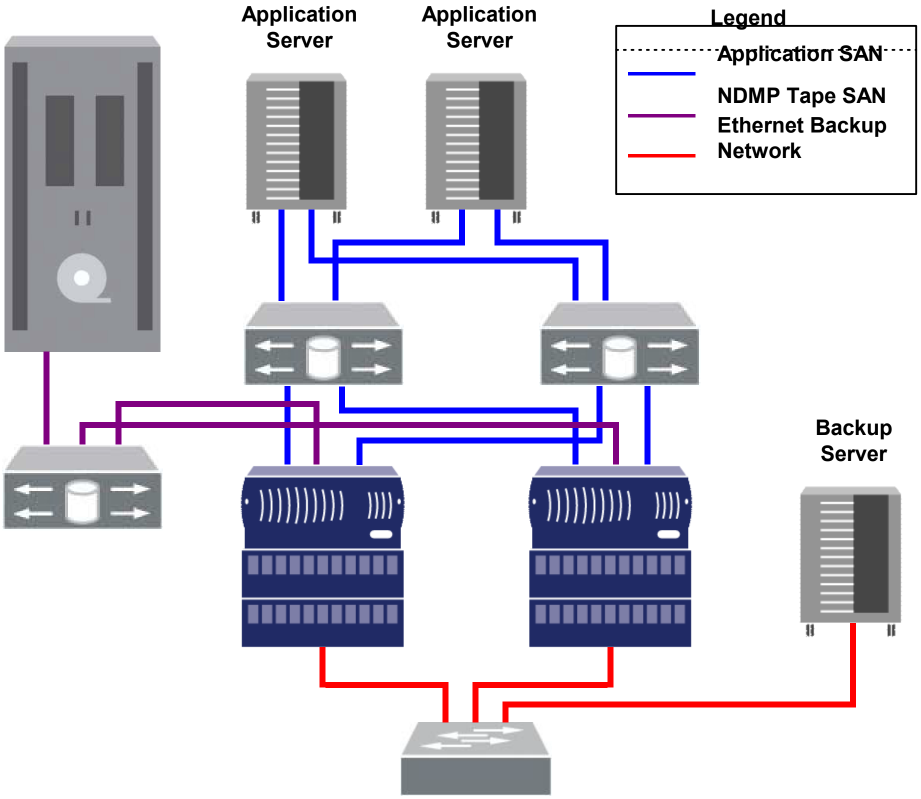

Figure 3) Controller-Based SAN Backup/Recovery Diagram

The above diagram depicts a SAN with two application servers and two controllers redundantly attached to two fabric switches, avoiding single points of failure. The controllers are also attached to a second SAN for tape backup. The backup server and the controllers are all connected to a private Ethernet network for controlling backup and recovery operations. Zoning can be configured to support attaching tape devices to the SAN if using a third switch is not desired.

The library and drives could alternatively be SCSI-attached to the controllers or attached via Gigabit Ethernet if an NDMP-compliant tape library is in use.

3.2.1. Snapshots

SnapMirror is often used for disaster recovery (DR) planning. Here, volumes containing LUNs would be mirrored asynchronously to a controller at a DR facility. Preferably, application servers would be mirrored to this facility as well. In the event that the DR facility needs to be made operational, applications can be switched over to the servers at the DR site and all application traffic directed to these servers as long as necessary to recover the primary site. Once the primary site is online, SnapMirror can be used to transfer the data efficiently back to the production controllers. After the production site takes over normal application operation again, SnapMirror transfers to the DR facility can resume without requiring a second baseline transfer.

SnapMirror can also be used for backup consolidation or offloading tape backup overhead from production servers. This facilitates centralized backup operations, reducing backup administrative requirements at remote locations. It can also dramatically reduce overhead from stressful backup operations caused by small backup windows on production controllers. Since backup operations are not occurring on the production systems, small backup windows are not as important.

3.2.4. SnapVault

SnapVault builds upon the NeApp SnapMirror software by providing greater flexibility in the retention of Snapshots on the destination. This makes SnapVault ideal for backing up or archiving Snapshots to a controller or NearStore device. SnapVault can be used in this manner to perform disk-based backups of LUNs to a second controller or NearStore appliance, greatly reducing the time to back up or recover these LUNs when compared to tape-based backup and recovery.

Keep in mind that SnapVault as well as all host-based methods can only back up and recover an entire LUN. SnapVault will work well with applications that maintain transaction logs, such as databases. The LUN is restored and then transaction logs are rolled forward to bring the LUN to the desired state.

With SnapVault, there can be two separate schedules maintained. One schedule controls creation of the Snapshots on the source controller. The second schedule controls transfer of these Snapshots to the destination controller and the amount of time to retain them. It is recommended that Snapshots on the source controllers be created manually when FCP data is contained on the file system. Scripts should be used to quiesce the application or place it in hot backup mode before creating a Snapshot. Once the Snapshot is created, the application should be returned to normal operation. The UNIX `cron` or Windows Task Scheduler service can then be used to execute these scripts at specified intervals.

3.2.5. NDMP and Native Tape Backup and Recovery

Tape backup and recovery operations of LUNs should generally only be performed on the controller for disaster recovery scenarios, for applications with transaction logging, or when combined with other controller -based data protection elements, such as SnapMirror and SnapVault. All tape operations local to the controller operate on the entire LUN and cannot interpret the data or file system within the LUN. Thus, LUNs can only be recovered to a specific point in time if transaction logs exist to roll forward. Where finer granularity is required, host-based backup and recovery must be used.

If the operator does not specify an existing Snapshot when performing a native or NDMP backup operation, the controller will create one before proceeding. This Snapshot will be deleted when the backup completes. When a file system contains FCP data, one should always specify a Snapshot that was created at a point in time when the data was consistent. As mentioned earlier, this is ideally done in a script by quiescing an application or placing it in hot Backup mode before creating the Snapshot. After Snapshot creation, normal application operation can resume and tape backup of the Snapshot can occur at any convenient time.

SnapMirror is often used for disaster recovery (DR) planning. Here, volumes containing LUNs would be mirrored asynchronously to a controller at a DR facility. Preferably, application servers would be mirrored to this facility as well. In the event that the DR facility needs to be made operational, applications can be switched over to the servers at the DR site and all application traffic directed to these servers as long as necessary to recover the primary site. Once the primary site is online, SnapMirror can be used to transfer the data efficiently back to the production controllers. After the production site takes over normal application operation again, SnapMirror transfers to the DR facility can resume without requiring a second baseline transfer.

SnapMirror can also be used for backup consolidation or offloading tape backup overhead from production servers. This facilitates centralized backup operations, reducing backup administrative requirements at remote locations. It can also dramatically reduce overhead from stressful backup operations caused by small backup windows on production controllers. Since backup operations are not occurring on the production systems, small backup windows are not as important.

3.2.4. SnapVault

SnapVault builds upon the NetApp SnapMirror software by providing greater flexibility in the retention of Snapshots on the destination. This makes SnapVault ideal for backing up or archiving Snapshots to a controller or NearStore device. SnapVault can be used in this manner to perform disk-based backups of LUNs to a second controller or NearStore appliance, greatly reducing the time to back up or recover these LUNs when compared to tape-based backup and recovery.

Keep in mind that SnapVault as well as all host-based methods can only back up and recover an entire LUN. SnapVault will work well with applications that maintain transaction logs, such as databases. The LUN is restored and then transaction logs are rolled forward to bring the LUN to the desired state.

With SnapVault, there can be two separate schedules maintained. One schedule controls creation of the Snapshots on the source controller. The second schedule controls transfer of these Snapshots to the destination controller and the amount of time to retain them. It is recommended that Snapshots on the source controllers be created manually when FCP data is contained on the file system. Scripts should be used to quiesce the application or place it in hot backup mode before creating a Snapshot. Once the Snapshot is created, the application should be returned to normal operation. The UNIX `cron` or Windows Task Scheduler service can then be used to execute these scripts at specified intervals.

3.2.5. NDMP and Native Tape Backup and Recovery

Tape backup and recovery operations of LUNs should generally only be performed on the controller for disaster recovery scenarios, for applications with transaction logging, or when combined with other controller -based data protection elements, such as SnapMirror and SnapVault. All tape operations local to the controller operate on the entire LUN and cannot interpret the data or file system within the LUN. Thus, LUNs can only be recovered to a specific point in time if transaction logs exist to roll forward. Where finer granularity is required, host-based backup and recovery must be used.

If the operator does not specify an existing Snapshot when performing a native or NDMP backup operation, the controller will create one before proceeding. This Snapshot will be deleted when the backup completes. When a file system contains FCP data, one should always specify a Snapshot that was created at a point in time when the data was consistent. As mentioned earlier, this is ideally done in a script by quiescing an application or placing it in hot Backup mode before creating the Snapshot. After Snapshot creation, normal application operation can resume and tape backup of the Snapshot can occur at any convenient time.

When attaching a controller to a Fibre Channel SAN for tape backup, it is necessary to first ensure that NetApp certifies the hardware and software in use. A complete list of certified configurations is available in the NetApp Data Protection portal. Redundant links to Fibre Channel switches and tape libraries are not currently supported by NetApp in a Fibre Channel tape SAN. Furthermore, a separate host bus adapter must be used in the controller for tape backup. This adapter must be attached to a separate Fibre Channel switch that contains only controllers, NearStore appliances, and certified tape libraries and tape drives. The backup server must either communicate with the tape library via NDMP, or have library robotic control attached directly to the backup server. Figure 3 in section 3.2 illustrates a Fibre Channel tape SAN with the tape library controlled over NDMP.

4. Summary

There are many methods to back up data stored on a controller via FCP. Host-based methods provide the finest granularity of data protection, allowing selective backup and recovery of data within a LUN. controller-based methods provide very fast and efficient disaster recovery solutions. There is no single best method meeting all data protection requirements. One must prioritize requirements and combine methods to meet and exceed these requirements.

Remember that data protection is a constantly changing thing. As needs and usage change, so must data protection policies and technologies. NetApp is committed to providing industry-leading data protection solutions now and in the future. As needs and technology change, NetApp will continue to exceed customer expectations, providing the constant data availability and absolute data integrity they rely upon for success.

5. References

NetApp Data Protection Portal
http://www.netapp.com/solutions/data_protection.html

Data Protection Solutions Overview
http://www.netapp.com/tech_library/3131.html

SnapMirror® and SnapRestore™: Advances in Snapshot™ Technology
http://www.netapp.com/tech_library/3043.html

Oracle9*I*™ for UNIX® – Backup and Recovery Using a NetApp Controller in a SAN Environment
http://www.netapp.com/tech_library/xxxx.html

Oracle9*i* for Windows – Backup and Recovery Using a NetApp Controller in a SAN Environment
http://www.netapp.com/tech_library/xxxx.html

Network Data Management Protocol home page
http://www.ndmp.org/

NetApp, Inc.

495 East Java Drive
Sunnyvale, CA 94089
www.netapp.com