



NETAPP TECHNICAL REPORT

NetApp Virtual File Manager

Protecting Your Data: Business Continuity and Disaster Recovery

Jai Desai, Network Appliance, Inc
November 2007 | TR-3634

ENABLING COMPREHENSIVE DATA MANAGEMENT SERVICES

This document provides an overview of how NetApp Virtual File Manager can be used to deploy an automated management policy to deliver comprehensive file management services. The NetApp Virtual File manager applications are described, and information is provided on how the automated management differs from other solutions available today.

1. Overview

1.1. Purpose of This Document

Network Appliance™ (NetApp) storage system software enables enterprise users to architect, highly available storage solutions for geographically diverse data centers, creating reliable business continuity (BC) and disaster recovery (DR) solutions for the enterprise. Businesses often find themselves deploying solutions that cannot eliminate major delays in resuming normal business operations after a disaster or an outage. The combination of SnapMirror® and VFM (Virtual File Manager), however, bridges this gap, and gives both system administrators and executives peace of mind. **The SnapMirror-VFM solutions allow recovery from disasters in minutes, not hours.**

To successfully implement a DR/BC strategy you need a clear understanding of the business definitions and requirements. This includes revenue losses for failure to invest properly in a DR/BC solution. This document outlines an overview of the business justification for creating these BC/DR solutions along with technical solutions and sample scenarios.

2. Network Appliance File Area Network Business Continuity and Disaster Recovery Solutions

2.1. Introduction

NetApp Virtual File Manager helps the storage architect to design and develop cost-effective business continuity and disaster recovery solutions.

2.2. Industry Definitions of BC/DR

The following are definitions of BC/DR according to well-known publications and groups in the storage industry.

Storage Magazine:

“Business continuance planning seeks to prevent interruption of mission-critical services, and to reestablish full functioning as swiftly and smoothly as possible.”

NYSE/NASD:

“...ensures a company can continue meeting its customer obligations following any business-disrupting event.”

United States Government:

“The Continuity of Operations capability shall provide a continuity infrastructure which, through preplanned devolution of authorities, responsibilities, and essential functions, ensures... the improvisation or emergency acquisition of the capability to perform work at an alternate work site until normal operations can be resumed...”

Disaster recovery is the ability of a site to recover from external events such as natural disasters, hardware failures, and human error. The ability to recover does not mean that there is no interruption or disruption of normal business operations. The recovery process takes time, and often involves failing over to a secondary site while the primary site is affected by the disaster. During this failover, end users and customers are redirected to the new site, and the time to recovery results in lost business.

Business continuity is the degree to which business operations can continue without disruption not only in the event of natural disasters but also during IT infrastructure component failures and power outages. Business continuity and effective business continuity planning are linked to overall business productivity, operational resiliency, and protection against loss of revenue.

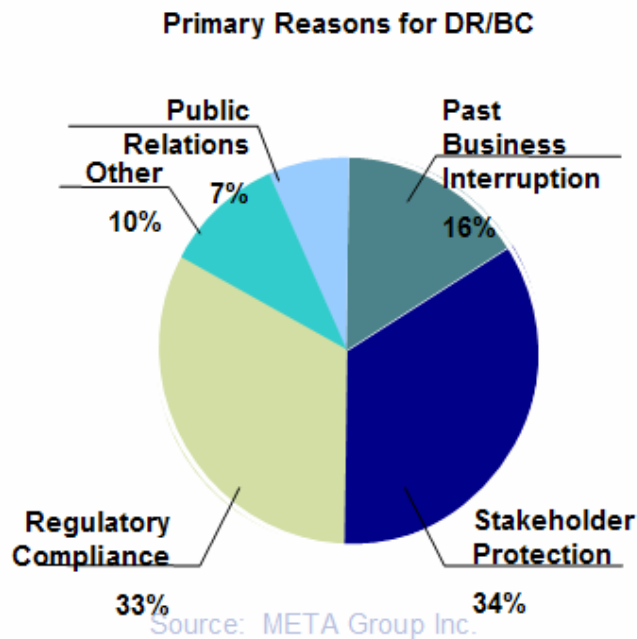
In order to maintain a sustainable business with multiple geographic locations, the IT department must maintain the same level of business availability for all sites, both before and after a disaster. What are the business motivations for investing in a strong, cost-effective DR/BC strategy?

2.3. **Business Motivations for Developing DR/BC**

If access to business information is disrupted, the potential loss is high. This loss can be measured in terms of diminished production, lower sales, longer product development cycles, and decreased revenue. As part of the motivation for developing a DR/BC strategy, businesses must:

- Understand different loss categories
- Take a financial approach to quantifying loss
- Focus on business service versus technology infrastructure
- Understand that availability is a mass-market requirement
- Understand customer expectations and how failure will affect market share and valuation

The chart below is based on research performed by the META Group, Inc., and outlines additional reasons to have a strong DR/BC strategy. Of special note is the requirement for regulatory compliance that is driving organizations to formulate a plan.



2.4. **Ensuring Business Continuity by Minimizing Time to Data**

For an IT manager, several approaches are available for using a BC/DR site to prevent disruption, minimize disruption, or repair business processes when an interruption occurs. These are:

1. PREVENT: Fault Tolerance = Embedded
The ability of a process and supporting components to withstand any type of error without interruption.
2. MINIMIZE: High Availability = Proactive
The degree to which a business process or component is operational and accessible when required for use.
3. REPAIR: Recovery = Reactive
The ability of a business to quickly resume everyday operations and recover its resources.

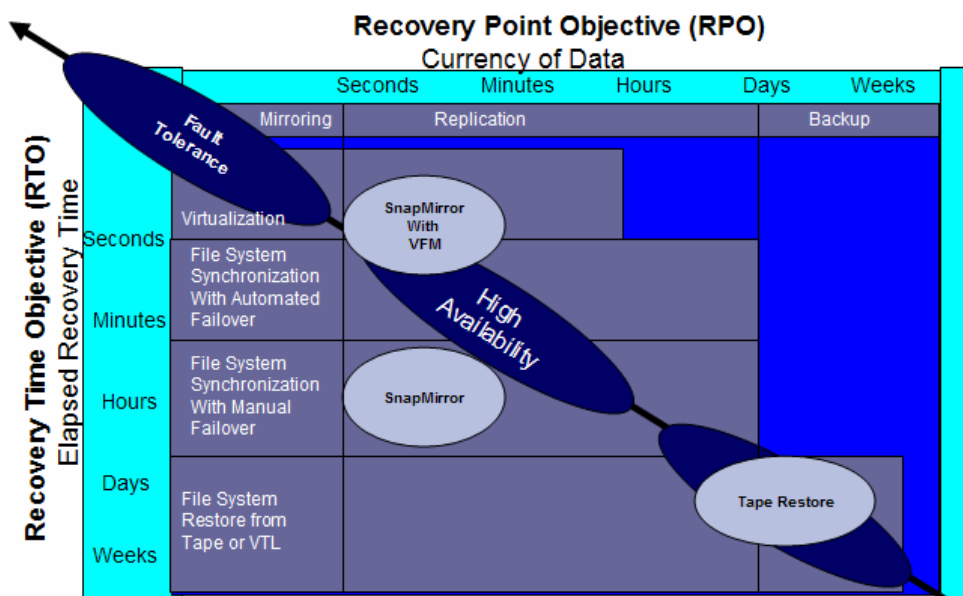
These goals are all met by using a solution with both NetApp Virtual File Manager and SnapMirror. Virtual File Manager, along with its many other features, provides storage administrators with policies that automate data management functions. This includes building and managing global namespaces and providing heterogeneous operating-system-independent migration (enabling local and remote replication). The Virtual File Manager global namespace provides a logical view of file data that is independent of its physical location. File data can be migrated seamlessly without disruption for user access. Likewise, user access to file data can be transparently directed to a replicated copy at a remote site.

One important feature that Virtual File Manager offers is close integration with SnapMirror. A combination of Virtual File Manager and SnapMirror provides quick recovery from a disaster.

SnapMirror provides the ability to replicate volume data from one NetApp appliance to another. Exceptionally powerful yet easy to use and administer, NetApp SnapMirror software delivers the disaster recovery and data distribution solution that today's global enterprises need. By replicating data at high speeds over a LAN or a WAN, SnapMirror software provides data availability and recovery for mission-critical applications. It continually updates the mirrored data to keep it current and available for disaster recovery, offloading tape backup, read-only data distribution, testing on nonproduction storage systems, online data migration, and more. If your enterprise is geographically dispersed and all locations need access to the same dataset, SnapMirror can distribute the same data to all locations. By automatically updating this data and allowing local access to mirrored data, SnapMirror can dramatically improve employee productivity and efficiency. NetApp SnapMirror software has many bandwidth-saving features that lower the infrastructure cost of data replication and disaster recovery. You can perform an initial full-volume transfer using tapes and then use the tapes to populate data in remote locations. After that, you need only update the new and changed blocks incrementally over the network.

While SnapMirror will replicate data to a BC/DR site, Virtual File Manager will synchronize file references and manage failover processes. After an outage or disaster occurs, user access to file data can be automatically redirected to the SnapMirror target and business continuity maintained.

There is no need to have users manually redirect access to the replicated data at the secondary site. The net result, as shown below, **provides recovery time in minutes, not hours.**



2.5. Maintaining Access to Data—Underlying BC/DR Technology Utilizing NetApp Virtual File Manager and SnapMirror

The following examines a variety of technologies used in designing a successful BC/DR strategy. First of all, a global namespace is used to virtualize geographically distributed files in a CIFS (Common Internet File System) environment or an NFS (Network File System) environment. This is a fundamental requirement for building a BC/DR strategy.

When establishing a global namespace, standard technologies must be used. CIFS with DFS (Distributed File System) is the technology of choice for Windows® environments and Automount is best suited for NFS environments. Virtual File Manager supports both of these technologies.

Looking at the architecture for BC/DR, the global namespace solution used with Virtual File Manager operates out of band, and is not in the line of data flow. There are several advantages to having an out-of-band approach for a global namespace. For example, if a failure occurs in the management software, access to the file system should remain available.

For a Microsoft® environment, Active Directory with DFS adds another dimension to fault tolerance (Virtual File Manager uses DFS in its global namespace implementation). When using Distributed File System with Active Directory, if one Active Directory domain controller fails, then another can easily take its place. Therefore, access to the virtual file links remains intact.

SnapMirror introduces a cost-effective, high-performance replication capability to the BC/DR process. Virtual File Manager will manage SnapMirror when a disaster occurs by breaking the mirror and failing over the logical file links in the global namespace, allowing virtually uninterrupted access to unstructured data during a failover. With both SnapMirror and Virtual File Manager in the solution, failures are managed quickly and automatically.

To summarize, Virtual File Manager and SnapMirror together:

- A) Manage the namespace using policies to control replication and creation of namespaces
- B) Virtualize the namespace by building logical file links not tied to physical hardware
- C) Make the secondary SnapMirror location writeable
- D) Fail over logical links when a disaster occurs at a physical location

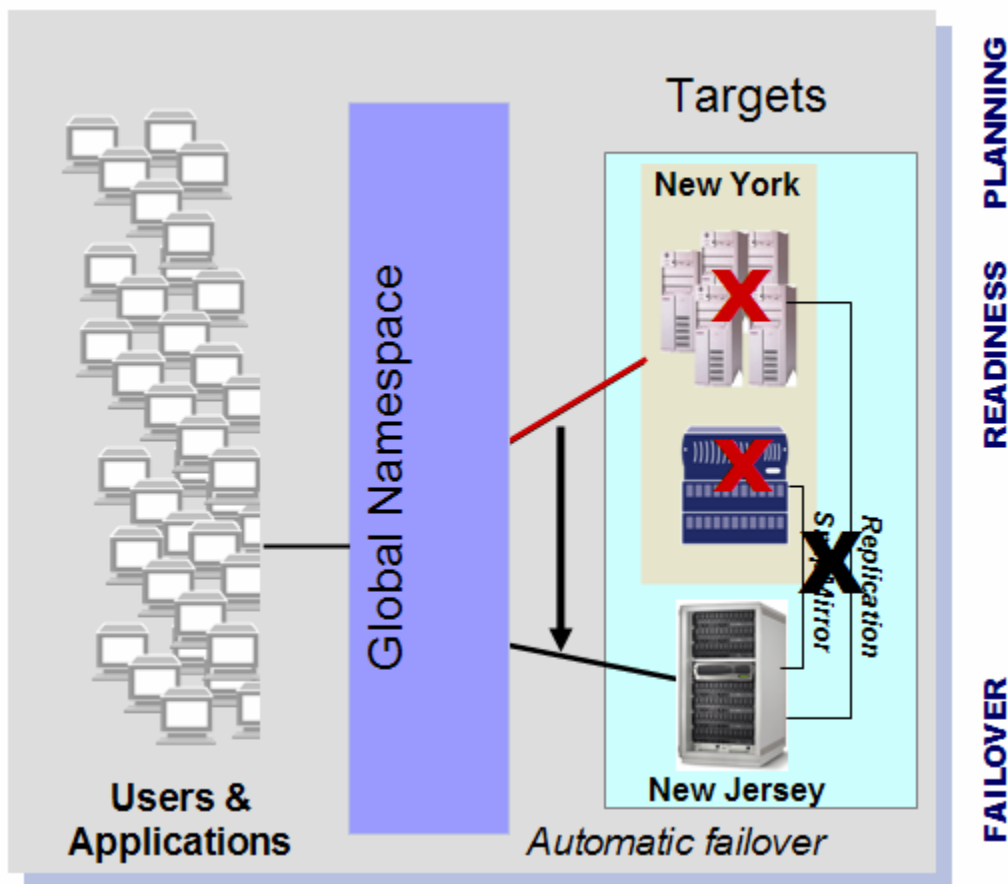
While the primary site is being recovered (DR), normal business operations can continue from the secondary site (BC).

SnapMirror provides a great disaster recovery solution, but SnapMirror and Virtual File Manager together go beyond disaster recovery to deliver a complete business continuity solution. The combination and synergy of SnapMirror and Virtual File Manager provide outstanding DR/BC value to customers.

2.6. Network Appliance Virtual File Manager and Business Continuity: an Example

In this example, there are two sites, one in New York and the second in New Jersey. The sequence of events for a DR/BC event is as follows:

- First, a network of storage is pooled using a global namespace. The global namespace makes file locations transparent to users and applications. This is done by using Virtual File Manager to create and manage the global namespace.
- Then SnapMirror is used to enable asynchronous replication (Virtual File Manager can be used for heterogeneous replication between Windows servers).
- If a disaster occurs, Virtual File Manager policies cease replication and make secondary devices active through close integration with Data ONTAP®.
- Automatic failover occurs between the sites, with client requests transparently redirected to the target device.

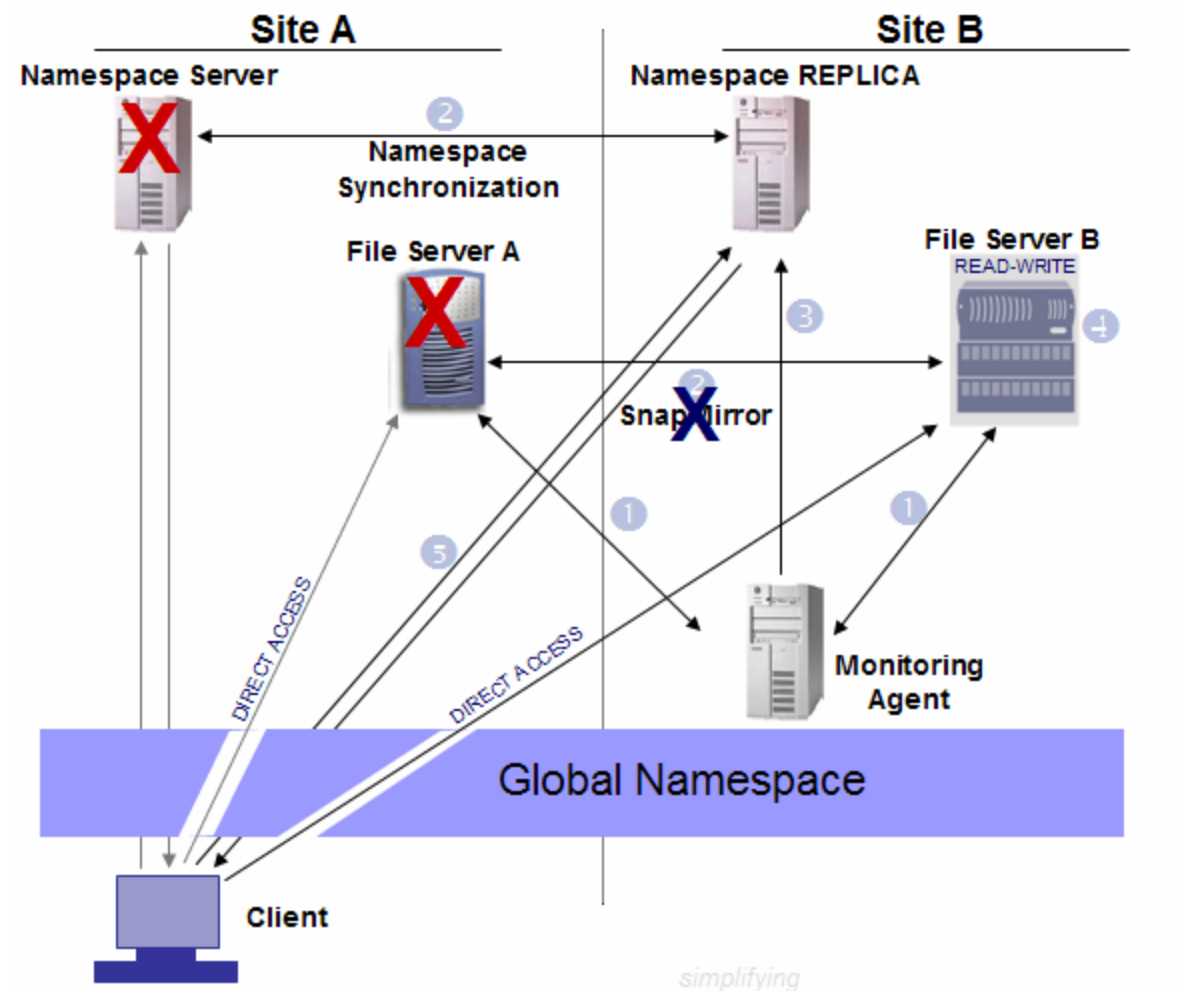


Using Virtual File Manager and SnapMirror at the data center and the remote DR sites, enterprises can create a coherent global file-serving environment that leverages centralized storage, management, and information lifecycle infrastructures.

2.7. How BC Works: Some Operational Details

The following are additional details regarding the way Virtual File Manager and SnapMirror provide business continuity during a disaster. By synchronizing the namespace between the primary site and the disaster recovery site, Virtual File Manager minimizes the time to data when a disaster occurs. This is accomplished using the following process:

1. Virtual File Manager monitors links to the file servers.
2. Then, Virtual File Manager synchronizes the namespace and SnapMirror synchronizes the data.
3. Once a site failure occurs, the monitoring agent detects the failure and updates the namespace.
4. Virtual File Manager automatically breaks the SnapMirror link, fails over the link to File Server B, and makes it read-write.
5. The client is now redirected (using a referral from CIFS and DFS) to File Server B.
6. Normal business operations continue while Site A is being recovered.

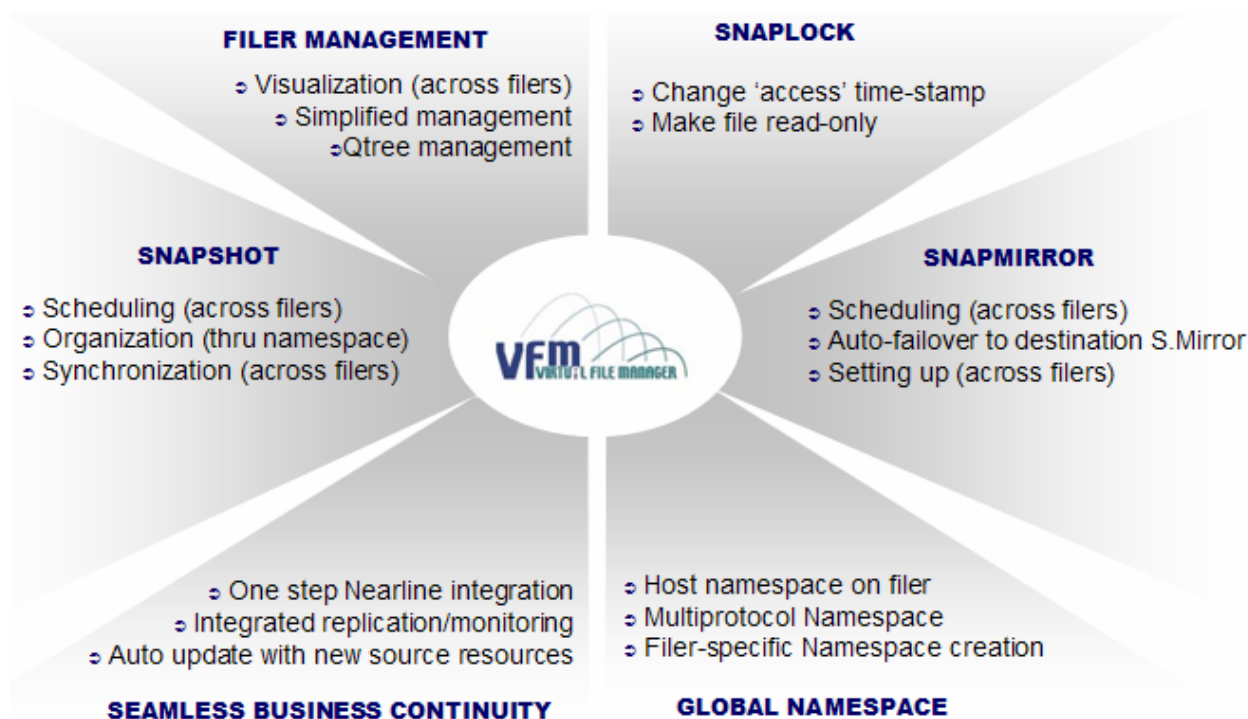


2.8. **Virtual File Manager Strengthens Snapshot™ functionality and SnapLock® for Backup Strategies with DR/BC**

To strengthen the DR strategy, a strong backup strategy is also required. Products such as Snapshot and SnapLock can be used to assist in a backup strategy. As noted below, by using Virtual File Manager along with Network Appliance Snapshot, SnapMirror, and SnapLock, a cost-effective DR/BC and backup solution can be implemented. Backups with consistent views of data can be taken using Snapshot and you can comply with regulatory and best-practices records-retention requirements with SnapLock. SnapLock allows the creation of non-writable, non-erasable WORM volumes, thereby preventing critical files from being altered or deleted until a specified retention date.

SnapLock allows WORM data to be replicated securely and automatically between multiple NetApp storage systems using NetApp SnapMirror software. WORM-to-WORM replication enables data at remote sites to fully comply with regulations or best practices, resulting in a highly robust WORM data protection solution. WORM data can also be backed up to tape for an additional level of data protection.

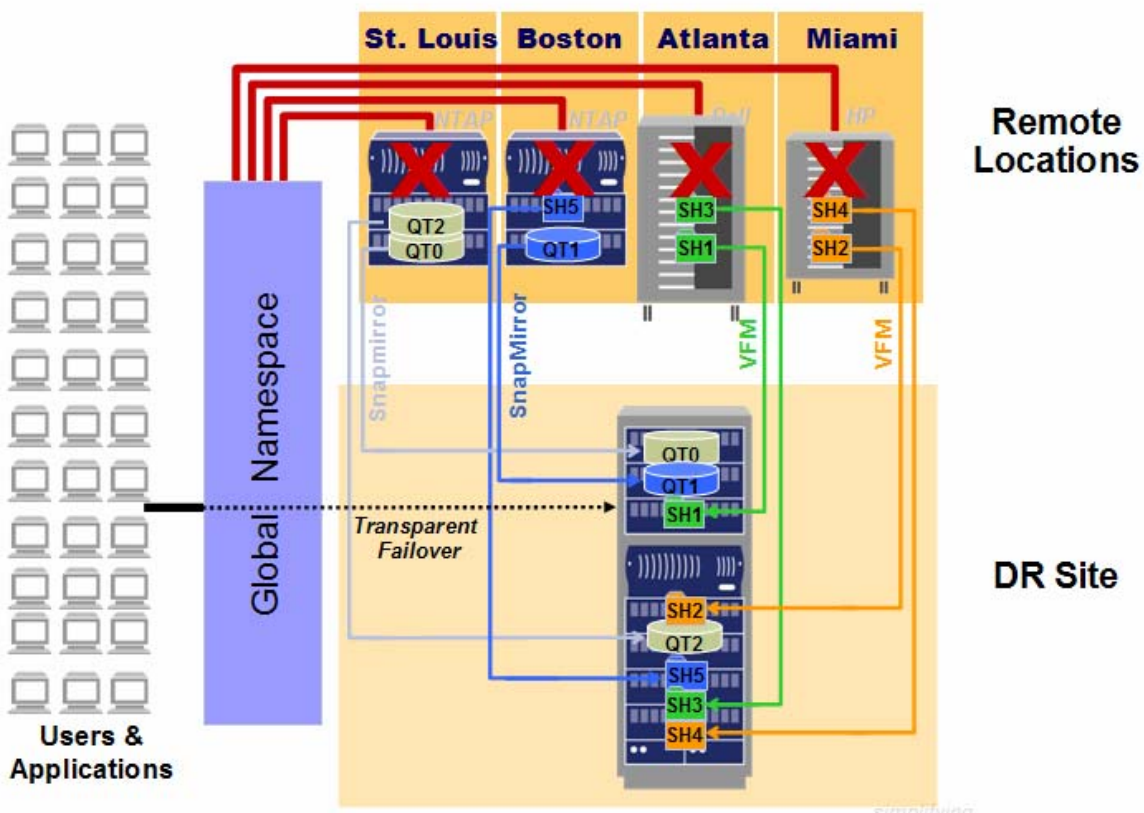
Virtual File Manager allows for fast, seamless failover to data stored on NetApp storage systems protected with SnapMirror.



3. Lowering BC/DR Costs by Using NearStore® and Virtual File Manager

As mentioned in the previous section, the first step in minimizing BC/DR costs is to use Virtual File Manager and SnapMirror to manage BC/DR. However, it can be expensive to build multiple DR sites, and most IT budgets cannot accommodate several secondary sites for each primary site. Therefore, it makes sense to consolidate the BC/DR site at one location. In addition, cost-effective NetApp NearStore storage systems can be used at the DR site for economy of scale if additional SnapMirror replication streams are required.

Below, four sites are consolidated at one BC/DR site. SnapMirror and Virtual File Manager are used to manage the failover process for all sites. This saves costs when purchasing and maintaining four identical BC/DR sites. Additionally, backup can be performed at the DR site, thus saving administrative and backup infrastructure costs for the overall operation.



4. Summary

NetApp offers several low-cost, easy-to-manage business continuity and disaster recovery solutions.

SnapMirror and Virtual File Manager provide a cost-effective, high-performance solution set for BC/DR. These solutions ensure that NetApp customers can quickly recover from a disaster as well as continue normal business operations while recovery takes place.