

# HP solutions with Microsoft VSS

## HP OpenView Storage Mirroring



Volume Shadow Copy Service .....	3
What Shadow Copies for Shared Folders does not do .....	4
Protecting the snapshots .....	6
Flexibility to meet your needs .....	8
For more information .....	9

---

Have you ever felt the frustration of having to spend hours or even days rebuilding files because of inadvertent changes, accidental deletions, or other mishaps?

---

You spend hours or days creating a document or presentation only to have it become corrupted or you inadvertently overwrite it with undesirable changes. Then, you spend the next few hours, or even days, recreating it, hoping that you can remember all that had gone into the original. If you are in IT, how many requests do you get from your end users for single file restorations? Add to that the worry about server and site failure, and you have quite a stressful life. Would it be nice if these issues were a thing of the past? Does the comfort of knowing that users can recover their own files and that your data is well protected against loss and failure seem inconceivable to you? Think how much more productive and stress-free your workday would be knowing that your data was fully protected from loss.

Using Microsoft's Volume Shadow Copy Service (VSS), Windows Storage Server 2003, and the strength of HP OpenView Storage Mirroring, you now have the products to achieve your goals to reduce downtime, protect your critical assets, and reduce time spent on restoring and rebuilding files and servers.

This white paper clarifies the strengths of both products and covers some of what they can and cannot do, as well as offers some insight into how you can protect your data, your time, and the time of others by implementing these two very complementary best-of-breed data protection solutions. This paper also answers the common question of whether VSS can be used in place of Storage Mirroring for your disaster recovery and replication needs.

While technical specifics of these solutions are not covered, the business benefits, high-level functionality, and implementation strategies for a few different scenarios are discussed. VSS provides several different methods and interfaces that allow it to work with VSS-enabled applications such as backup and VSS-enabled hardware-based snapshot and clone technologies. This white paper does not cover these functions but rather focuses on the software snapshot capabilities shipped in Windows Server 2003.

So, does VSS replace Storage Mirroring for disaster recovery and replication services? No, it does not. Microsoft clearly states that VSS does not replace backup or replication/disaster recovery solutions. In fact, the combination of VSS and Storage Mirroring provides a very complementary solution.

VSS native software snapshot support provides point-in-time copies of volumes at the local server. These software snapshots are not "transportable," meaning the point-in-time copies cannot be created on a remote server nor made accessible from a remote machine at your disaster recovery site. Storage Mirroring is the industry-leading local and long-distance host-based replication software solution that bridges the gap between local and remote copies of data.

## Volume Shadow Copy Service

With the release of Windows Server 2003 and Windows Storage Server 2003, Microsoft introduced an exciting and valuable infrastructure to its already robust operating system—VSS. VSS enables the creation of snapshots, or point-in-time copies of volumes. These snapshots are images of the data as it looks at a particular instance in time. By maintaining these timely images of data, users and administrators can quickly recover individual files or whole volumes directly from disk as they appeared at the time the snapshot was taken.

Microsoft shipped a feature in Windows Server 2003 called Shadow Copies for Shared Folders that uses the VSS infrastructure to enable users to restore files on their own, without administrator intervention. By including this feature with its operating systems, Microsoft has dramatically reduced one of the most common time-consuming tasks for both end users and system administrators: single file recovery. Inadvertent changes, deletions, and corruption are just a few of the reasons files might need to be restored or rebuilt. Recreating files is not only time-consuming and inefficient but often results in lost data and incomplete files after the restore or rebuild. Restoring a file from tape can often provide you with a copy of the file as of last night, assuming the backup completed. However, this consumes the time of the system administration staff and usually takes at least a day, often longer, to get the file back, as tapes might need to be retrieved from offsite retention.

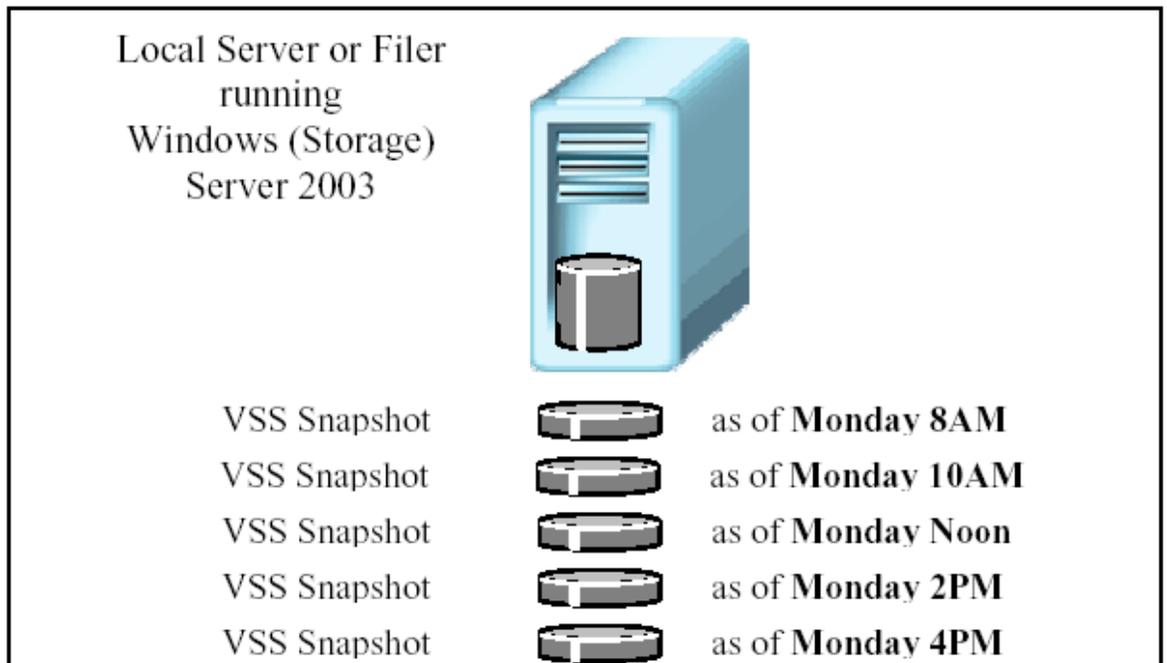
Microsoft now provides a native solution for this with Shadow Copies for Shared Folders. By taking scheduled periodic snapshots, Shadow Copies for Shared Folders allows end users to recover files on their own, without the need to involve IT or to retrieve and mount a tape. Should users delete or make undesirable changes to documents, they can select the files from any desired snapshot and replace them with up to 64 previous versions. They can select one from one hour ago, five hours ago, or maybe a week ago, which is all possible depending on the Shadow Copies for Shared Folders configuration settings.

Administrators can configure Shadow Copies for Shared Folders to create point-in-time snapshots of particular volumes, which users can then access directly should they need to recover a file. The ability to define the frequency of the snapshots allows for Shadow Copies for Shared Folders to be customized to meet your specific needs. Not only can Shadow Copies for Shared Folders improve file recovery processes, but it can also enhance other standard processes, such as backup and archival.

Shadow Copies for Shared Folders provides a self-service file recovery mechanism to end users. Through Windows Explorer, users can easily view the available snapshots and select their files from any point in time they choose. The chosen files are then taken from the selected point in time and copied to their personal folder. Shadow Copies for Shared Folders can be configured with up to 64 different snapshots for each volume, ensuring the right file is available when needed. Variables such as criticality of the data and the frequency of change to the data should be considered when determining the schedule for snapshots to be taken. By taking an hourly snapshot, for example, users can recover a file from the desired timeframe by themselves, without involving the IT staff and without the need to retrieve and mount any tapes. Plus the biggest benefit is the file is at most one hour old, whereas recovery from tape would likely be from the previous day at a minimum, and often older. However, depending on the size of the snapshots, creating them hourly might not allow them to be available for as long as your business requires as older versions are purged when the allocated space for Shadow Copies for Shared Folders is used.

Enhanced backup using VSS-aware backup software can greatly enhance the quality of your backups. Backing up the snapshots ensures that there are no open file conflicts that can result in incomplete backups.

Figure 1. VSS snapshots



## What Shadow Copies for Shared Folders does not do

Although Shadow Copies for Shared Folders provides an excellent way to recover files and minimize lost work due to deleted files or unwanted changes, what if the disk, server, or site were to become unavailable? And what about those files and applications that cannot afford **any** lost data, requiring up-to-the-minute recovery? VSS software snapshots are not available to restore from if the server or disk becomes unavailable as the original source disk must be available and in tact.

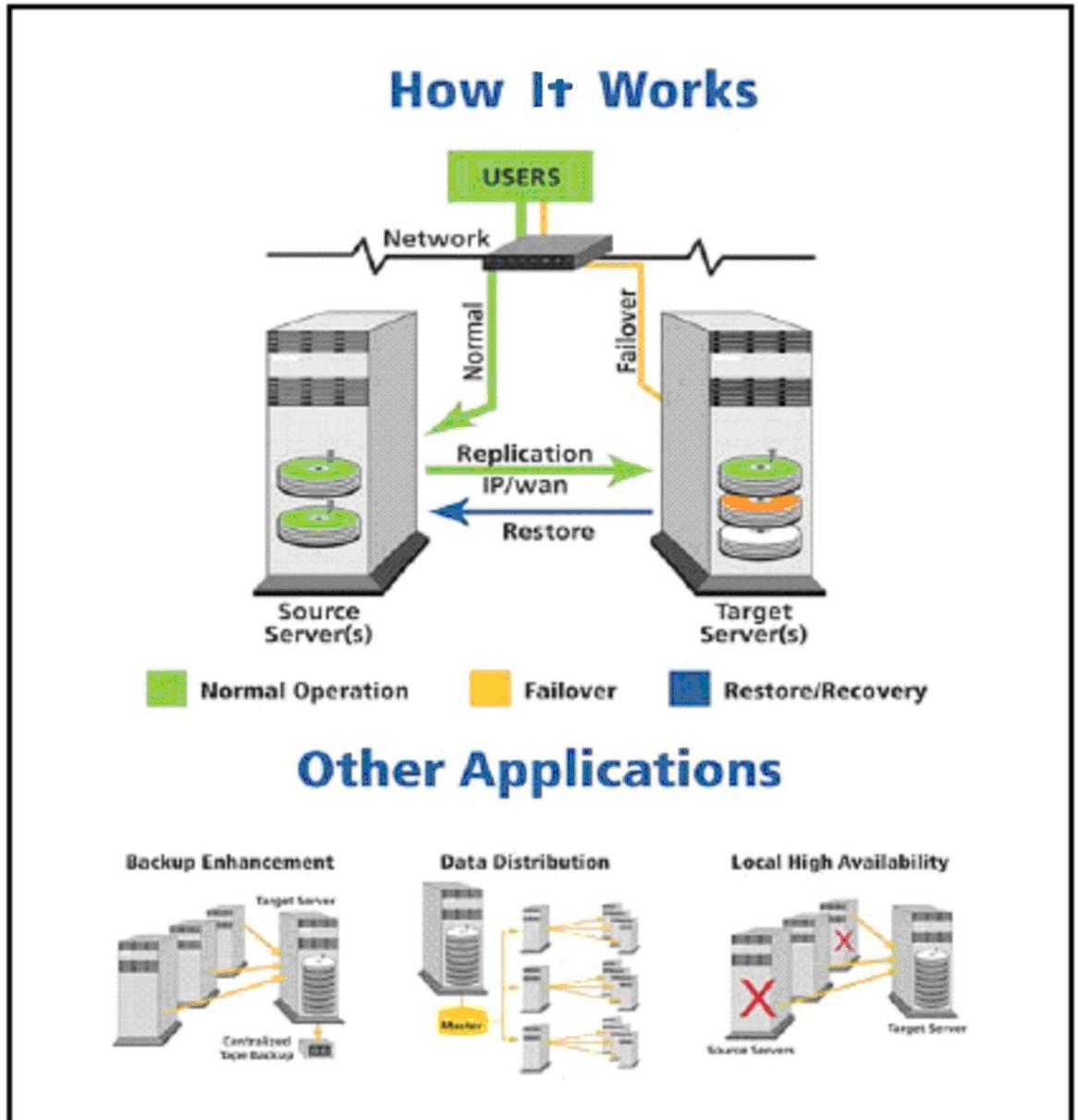
Disaster recovery is generally considered the ability to recover your data in the event of a local or regional failure. Some regulations require a minimum distance of 200 km between the production data and the remote copy. As native VSS software snapshots are not transportable, native VSS software snapshots are not designed to solve disaster recovery needs. While local snapshots allow for a quick recovery of files from different points in time, the snapshots would be unavailable for recovery in the event of a disk, server, or site failure.

HP offers Storage Mirroring, an industry-leading host-based replication software, to provide solutions for disaster recovery needs. One of the strengths of HP replication technology is that it protects files at the byte level, regardless of the application or physical storage device it is running on. Data changes are captured as they occur and replicated in real time over existing IP networks to a separate (local or remote) server. This process ensures the data on the target or remote system is as current as the production data.

By using Storage Mirroring, the data at the local site can be replicated in real time to a remote site, either across town, to the next state, across the country, or across the globe, ensuring your data is available should a local or regional failure occur. For enhanced protection or for data distribution, Storage Mirroring can replicate the local data to numerous remote sites simultaneously by implementing a one-to-many configuration. Since Storage Mirroring replicates asynchronously and copies just the byte-level changes, the performance impact to your applications and network is minimal.

Since Storage Mirroring works at the file-system level, it can replicate any data, whether they are flat files or database files such as Exchange or Microsoft SQL Server. Since most companies' critical data reside in some database, this is a critical aspect to consider when implementing your disaster recovery solution. Storage Mirroring is hardware independent and can be used to replicate between any Windows storage device.

Figure 2.



Another aspect to consider is your Recovery Point Objective (RPO). RPO is the amount of data (in days, hours, minutes, and seconds) that your business can afford to lose in the event of a failure. For example, if the server fails at 12:00 PM, how far back is acceptable to recover from? One hour, five hours, immediate? Since VSS software snapshots are not available in the case of a server or drive failure, you would still be required to go back to the latest tape backup to rebuild an entire disk. Not only is this a very time-consuming exercise, it may not meet your defined RPO. You will also lose all the previous point-in-time snapshots so you can no longer recover files from a previous point in time.

With Storage Mirroring, the replication process is continuous and real-time, resulting in up-to-the-minute recovery. As Storage Mirroring replicates to another disk, it enables restoration of the copy after the disk is rebuilt. There is no need to retrieve and mount tapes and apply incremental changes, resulting in rapid recovery with minimal or no data loss. For an even faster time to recover, you can restore to a different disk or server instead of waiting for the production server to be rebuilt. You can even have the target server stand in for the failed server using the built-in failover mechanism in Storage Mirroring, which allows for the target server to assume the name and IP address of the production server, allowing for a very rapid return-to-business for your users. In many cases, users are not even aware there was a failure.

So far, this paper has discussed snapshots to protect against file corruption and deletion by using Shadow Copies for Shared Folders and remote replication for protection from server, site, and regional failures. You should understand some of the value and benefits of Shadow Copies for Shared Folders and Storage Mirroring on their own, but what if both products are combined into a single solution?

## Protecting the snapshots

While having multiple copies of files on the local server provides for excellent recoverability should the file become corrupt, have unwanted changes, or be deleted, what protects those software snapshots in the event of a disk or server failure, or a power failure or regional failure? The software snapshots are as vulnerable as the original copies. Should the server or site suffer a failure, the originals **and** software snapshots are no longer available. You will have to restore all your data from the latest tape backup, which is timely and has a poor RPO. For this reason, your data protection solution should include plans to maintain snapshots of the replicated data at the remote sites.

With Storage Mirroring replicating your production data, should a local server failure occur you could recover the data from the remote Storage Mirroring replica and rebuild the server to the state it was in when it crashed. However, users would no longer be able to restore a file from a previous point in time, as all the snapshots were lost with the server failure. To retain point-in-time recoverability, the snapshots should be protected offsite as well as the original data. Since the Shadow Copies for Shared Folders snapshots are not actually full images of the original data, only the changes, it is not possible to replicate the snapshots from production to the target. Instead, replicate the production data to a target server using Storage Mirroring and enable Shadow Copies for Shared Folders snapshots on these replicas. To attain this level of protection the following configuration could be implemented:

- Implement Storage Mirroring to replicate your production data remotely for disaster recovery purposes
- Implement Shadow Copies for Shared Folders snapshots on the local volumes and shares as necessary, providing users with a self-service way to recover their files should they have undesired changes or be accidentally deleted
- Implement Shadow Copies for Shared Folders on the remote Storage Mirroring replicas to create point-in-time copies at the remote site

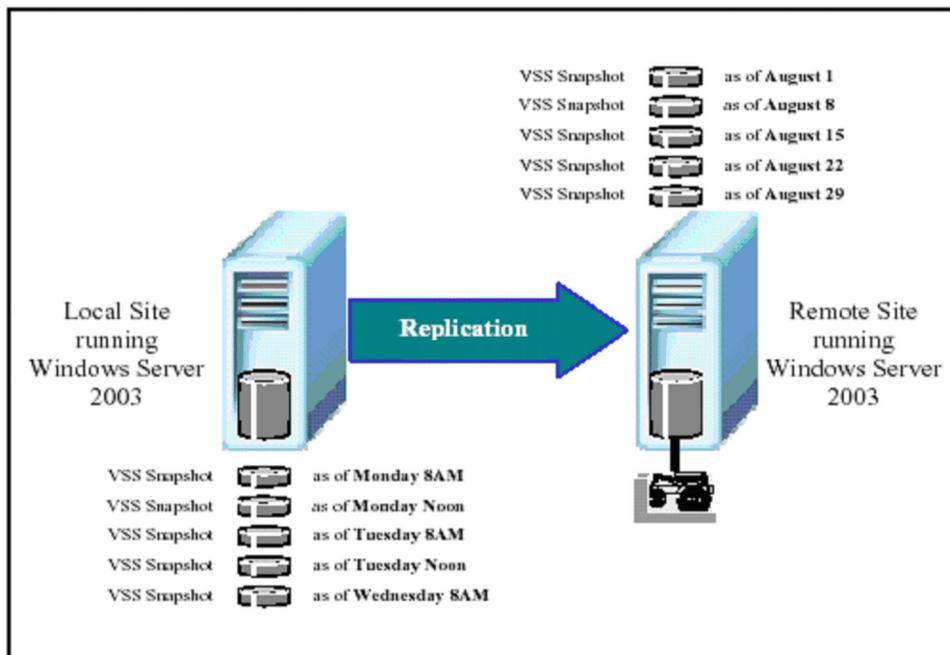
This configuration provides you with remote up-to-the-minute replicas for recovery from a failure at the local site, local snapshots for quick file restoration, and remote snapshots to maintain your ability to recover files from a previous point in time should the production server fail and lose the local Shadow Copies for Shared Folders snapshots.

Now, should a local failure occur, causing loss of the production data **and** the local Shadow Copies for Shared Folders snapshots, you can rebuild the server by way of the Storage Mirroring replicas to the state immediately preceding the failure. If users require a file from before the failure time, they can still restore it from the Shadow Copies for Shared Folders snapshots on the remote server. When the local server is rebuilt, Shadow Copies for Shared Folders should again be enabled to resume taking local Shadow Copies for Shared Folders snapshots. Should a file be desired from before the failure, the remote site will continue to make that data available using the Shadow Copies for Shared Folders

snapshots that were taken before the production disk failure. From the target server, select the files to recover using the Previous Versions client provided by Microsoft (as previously described), recover them to the target server, then copy them back to the production server, or anywhere else you desire, using standard Windows copy methods (Figure 3).

Shadow Copies for Shared Folders is enabled locally to create snapshots at 8:00 AM and 12:00 PM for file recoverability, allowing users to restore their own files. Storage Mirroring is replicating the production data (not the snapshots) from the local site to the remote disaster recovery site. Shadow Copies for Shared Folders is configured on the remote site to create a weekly snapshot for recovery in the event of a failure at the local site.

**Figure 3.** Storage Mirroring and Shadow Copies for Shared Folders



Do you want the benefits of creating software snapshots for data residing on Windows NT® and Windows 2000 without having to upgrade to Windows Server 2003? Although this is not natively possible on these operating systems (since VSS is not available), you can still achieve snapshot capabilities without having to upgrade them. Since Storage Mirroring supports both Windows NT and Windows 2000, you can configure replication from those servers to a new or existing Windows Server (or Storage Server) 2003 server and enable Shadow Copies for Shared Folders on those replicas. Should a file need to be recovered, you can restore it from the Shadow Copies for Shared Folders snapshot on the target Windows Server 2003 server.

Also note that if you are running Windows Powered NAS, you can also achieve the same benefits as with Shadow Copies for Shared Folders. Although not called Shadow Copies for Shared Folders, Windows Powered NAS has snapshot capabilities included that can be used in conjunction with Storage Mirroring to provide the same solutions described throughout this document.

## Flexibility to meet your needs

As you can see, the specific configuration options are virtually limitless and can meet most any business requirements. For example, to improve your recovery process you might want to keep one day's worth of hourly software snapshots and a weekly software snapshot (all stored on disk, locally, remotely, or both) for immediate availability and recoverability. Almost any other disaster recovery and data availability scenarios you require are equally possible and practical with Shadow Copies for Shared Folders and Storage Mirroring.

Is centralized backup in your plans? Now you can reduce software, hardware, and management costs at regional locations and maintain control and quality from the central data center by replicating that data locally using Storage Mirroring and perform the backup from there. Remember to configure Shadow Copies for Shared Folders on the remote office servers to allow users to recover files on their own.

Together, Microsoft and HP Software can offer you an even greater level of protection and flexibility, ensuring that you have the solutions necessary to meet and exceed your service level, business, and regulatory requirements. When considering enterprise technologies, it can be difficult to select vendors that support large areas of the organization. When considering applications (such as Exchange, Microsoft SQL Server, Oracle®, and file services) into their various versions, the task is even more daunting. However, because HP OpenView Storage Mirroring focuses on files and not applications, the same level of data protection is available for Exchange, Microsoft SQL Server, and most other Windows-based applications. More simply put, you can standardize on one Windows availability solution, regardless of the myriad applications in your environment.

## For more information

HP Storage Products:

<http://welcome.hp.com/country/us/en/prodserv/storage.html>

HP Storage Software:

<http://h18006.www1.hp.com/storage/software.html>

HP OpenView Storage Mirroring:

<http://h18006.www1.hp.com/products/storage/software/sm/index.html>

© 2004 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft, Windows, and Windows NT are U.S. registered trademarks of Microsoft Corporation. Oracle is a registered US trademark of Oracle Corporation, Redwood City, California.

5982-6827EN, 06/2004

