



Windows Server 2003 Active Directory Fast Recovery with Volume Shadow Copy Service and Virtual Disk Service

Microsoft Corporation
Published: August 2003

Abstract

Using the new Microsoft® Windows Server™ 2003 services of Volume Shadow Copy Service and Virtual Disk Service, it is now possible to recover failed Microsoft® Active Directory® servers in minutes rather than the hours that previous recovery methods required.

This paper supplies a fast recovery demonstration designed to enable system administrators to implement their own fast recovery solutions in their own Active Directory environments.

Contents

Introduction	1
Active Directory	1
Protecting Active Directory Information.....	1
Potential Problems	1
Limitations to Tape Backups	2
Fast Recovery in Windows Server 2003.....	2
Volume Shadow Copy Service.....	2
Virtual Disk Service	3
Fast Recovery.....	4
Timeline.....	4
Mechanisms Underlying Fast Recovery.....	5
Shadow Copy Creation	5
“Transport” through LUN Masking and Unmasking.....	5
Boot from SAN.....	6
Fast Recovery Demonstration	7
Summary of Results	7
Streamlined Recovery Management.....	7
Faster Time to Restore.....	8
Demonstration Configuration	8
Servers	8
Storage	9
Interconnects	9
Steps to Enable Fast Recovery	11
Prior to System Failure.....	11
Initial System Setup (T ₀).....	11
Backup (T ₁).....	12
Post System Failure	13
Restore Data (T ₃)	14
Resynchronize Data (T ₄)	15
Return to Production (T ₅)	15
Conclusion	16
Related Resources	17

Introduction

Microsoft Windows® Server™ 2003 has two new storage services, the Volume Shadow Copy Service and the Virtual Disk Service. Using these new services, storage array vendors and backup software vendors are able to develop new solutions that allow system administrators to significantly improve recovery procedures in their environment.

With the combination of Windows Server 2003, Storage Area Network (SAN) attached storage arrays, and new versions of backup applications, it is now possible for a system administrator to implement fast recovery of Active Directory servers. This paper includes a demonstration on how to maximize the benefits of using the Volume Shadow Copy Service and the Virtual Disk Service for fast recovery of Active Directory servers.

Active Directory

Microsoft® Active Directory® directory service, enhanced in Windows Server 2003, is the directory service for the Windows operating system. Active Directory provides a place to store information about objects on the network, such as users, computers, files, printers and applications. It provides a consistent way to name, describe, locate, access and secure information across distributed computer systems, thus simplifying system administration, strengthening security, and extending interoperability.

Directory information is stored on servers known as domain controllers. These domain controllers are accessed across the network by users, applications or other services, both to store information and to query the directory database for information.

Mid-sized organizations can have tens of thousands of objects, most of which are users, stored in Active Directory; enterprise-sized organizations can have hundreds of thousands or millions of objects.

Protecting Active Directory Information

If Active Directory information becomes corrupt, users might not be able to log in and access network resources. As a best practice, deploy Active Directory servers on three volumes: the operating system volume, the Active Directory database information volume, and the Active Directory log files volume. Active Directory is backed up as part of System State, which includes the database, log files, registry, system boot files, COM+ registration database, and Sysvol. Therefore, it is critical that these volumes be backed up and restored as a set.

Potential Problems

Active Directory information must be protected against a number of potential problems:

- **Hardware Failure.** To protect against problems that result in disk or other hardware failure, it is recommended that an organization use a combination of fault tolerant protected volumes (using either mirroring or RAID-5), and at least two domain controllers in each Active Directory domain. These domain controllers act as peers sharing the Active Directory workload; however, if the hardware fails in one server, the second server, with its replicated copy of the data, continues to provide necessary services. Note that, when there is an outage of one server in a configuration that has only two Active Directory servers, the remaining server is a single point of failure for the duration of the outage.
- **Data Corruption.** While mirroring and RAID-5 configurations provide fault tolerance for potential hardware failures, these solutions do not protect against data corruption, because the mirrored copy of data is damaged along with the original copy. Potential data loss or corruption issues traditionally require a single point-in-time backup copy of all volumes, and it

is necessary to keep this backup physically separate from the original. Using a tape archive backup solution has been the preferred method for implementing recovery procedures for these kinds of failures.

Limitations to Tape Backups

Tape backups are time intensive and impact server performance, and therefore tend to be done relatively infrequently (full backups are usually done only once a week). In addition to this drawback, there are a number of other others, including:

- A time intensive tape restore process.
- A time intensive resynchronization process. The longer the tape restore process, the greater the divergence between the shadow copies and the online Active Directory server(s) that continue to write transactions to disk.
- Decreased performance of the remaining Active Directory server(s) because it now carries an increased workload.

Fast Recovery in Windows Server 2003

A highly effective alternative to traditional tape-based protection is to make point-in-time shadow copies. Use of point-in-time shadow copies with Active Directory configurations allows rapid recovery from a number of specific system problems, including:

- Bad service pack installation.
- A third party component, such as an application agent, filter driver, or device driver, that has rendered the system unusable or unstable.
- Corruption of the system registry.
- A virus that has affected a system component.

Because this mirroring (or “cloning”) process is fast and non-disruptive to system performance, shadow copies can be made more frequently than tape backups. Shadow copies kept locally on a storage area network can be quickly accessed; with the appropriate hardware provider, they can be transported to a backup server, backed up to tape, and sent to offsite storage for archiving.

With the Volume Shadow Copy Service and the Virtual Disk Service, Windows Server 2003 contains new functionality to enable fast data restores, cutting restore time from the hours it can take with tape backups to just minutes. Since the restore time is so much faster, correspondingly fewer Active Directory changes can occur. This shortens resynchronization times considerably, enabling the machine to return to production significantly faster.

Volume Shadow Copy Service

Volume Shadow Copy Service supports creation of high fidelity single point-in-time shadow copies—also known as snapshots—of single or multiple volumes without impacting production server performance. Used for managing data, from Direct Attached Storage (DAS) to Storage Area Networks (SANs), Volume Shadow Copy Service coordinates with business applications, backup applications, and storage hardware to enable application-aware data management. Volume Shadow Copy Service also supports backups of open files.

Volume Shadow Copy Service coordinates the three software components necessary to create full-mirror shadow copies for fast restores:

- The utility that requests the creation of a shadow copy; also known as the “requestor.”
- Application-specific software that acts to ensure that application data is ready for shadow copy creation; also known as the “writer.” In this case, the writer is specific to Active Directory and ships in-box with Windows Server 2003.

- The interface that provides the functionality to actually make the shadow copy; also known as the “provider.” Volume Shadow Copy Service can create shadow copies by using either the (in-box) software provider, or a third party vendor hardware provider.

In a shared storage SAN configuration where there is often the need to make the data of one server accessible by another, a shadow copy of the original data can be transported “unmasked” to another server for use. This solution requires a hardware provider with transport capabilities. See details later in this paper.

Virtual Disk Service

Virtual Disk Service supports volume management functionality, provides a single Windows interface through which to manage multi-vendor storage devices, and provides application programming interfaces for independent software and hardware vendors to use to develop storage solutions. Much of the Virtual Disk Service functionality currently lies with two command line utilities, DiskPart.exe and Diskraid.exe. The **Diskpart** command set is used to control the creation, extension, deletion of partitions on both basic and dynamic disks. **Diskraid**, available through the *Windows Server 2003 Deployment Kit*, is used to configure hardware RAID subsystems with hardware providers; specifically to create, delete, extend and unmask *logical units*¹ (LUs) on the storage area network.

In the event of data corruption, Virtual Disk Service provides the functionality to make the backup shadow copies of uncorrupted volumes available for use. Virtual Disk Service does this by unmasking backup shadow copies stored on the SAN, thus making them visible to the server with the corrupted data; changing the read-only status to read/write; and, lastly, mounting the volumes on the server for use. This entire process is referred to as transport; the process, however, is virtual rather than physical, since the data is at all times on the storage array.

¹ A logical unit is a conceptual division (a subunit) of a storage disk or a set of disks. Logical units can directly correspond to a volume drive (for example, C: can be a logical unit). Each logical unit has an address, known as the logical unit number (LUN), which allows it to be uniquely identified.

Fast Recovery

As with tape-based recovery of data, recovery using Volume Shadow Copy Service and Virtual Disk Service requires planning well ahead of the actual server failure. The difference is that the data recovery from tape is far slower and more labor intensive than when using Windows Server 2003 technology and storage area networks, as outlined in the Timeline section. The specific steps for deployment are discussed in the “Steps to Enable Fast Recovery” section of this white paper.

Timeline

Figure 1 shows the timeline for backup, failure and recovery. Traditional backup methods are shown with the solid arrows. Best practice methods using Volume Shadow Copy Service, Virtual Disk Service and SAN technologies are shown with dashed arrows; time is indicated as T^i .

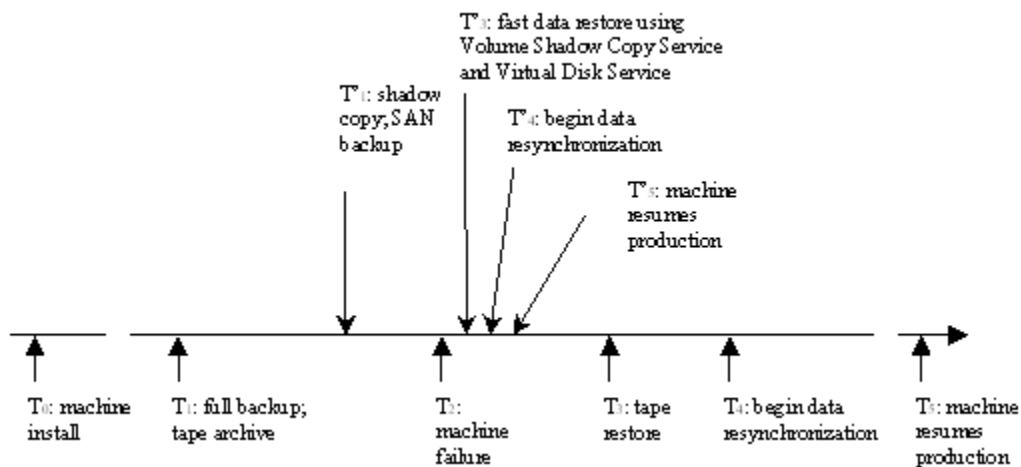


Figure 1. Timeline for Backup, Failure and Recovery

- T₀.** Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; or Windows Server 2003, Datacenter Edition, is installed using a LUN in the storage array according to vendor’s “Boot from SAN” guidelines. The server is then promoted to a domain controller. In order for Volume Shadow Copy Service and Virtual Disk Service solutions to work, the appropriate requestors, writers and providers must be installed on the host servers and the backup systems as per installation instructions from the vendor. For this scenario, assume three servers: two domain controllers providing redundancy and one providing backup capabilities. On the timeline in Figure 1, this first critical step in best practice backups occurs at time T_0 .
- T₁** Once Volume Shadow Copy Service and Virtual Disk Service components are installed, shadow copying as a backup strategy (T_1') is enabled. Because the shadow copy process is fast and non-disruptive to system performance, shadow copies can be made more frequently than with the traditional full backup method (T_1).
- T₂** Given loss of the primary server at T_2 , the secondary server assumes 100% of the client load, and operations continue using the replicated copy of the data, albeit with diminished performance and now a single point of failure. The highest priority of the system administrator is to restore the failed server to production as quickly as possible.

- T₃** With the shadow copy backup residing on the SAN, data restoration can begin immediately (T'_3), without the time intensive steps of retrieving tapes from an offsite storage vault (T_3). This minimizes data divergence, reduces the time that the remaining server must bear increased I/O load and pose a potential hazard as a single point of failure, and minimizes the impact on business bottom lines.
- T₄** Resynchronization (T'_4) thus begins much sooner than with tape restores (T_4), and is completed more quickly, since fewer changes to the data are possible, returning the machine to production (T'_5) in minutes as opposed to the hour or more it can take with traditional backup and restore methods (T_5).

Mechanisms Underlying Fast Recovery

The following sections briefly outline the conceptual aspects of each of these fast recovery solution components in a scenario in which Active Directory is installed on two servers with SAN attached storage. See Figure 3 for test configuration.

Shadow Copy Creation

The process of creating shadow copies begins when the backup application (requestor) contacts the Volume Shadow Copy Service to request a copy of the System State volumes. Volume Shadow Copy Service, acting as coordinator, notifies each of the System State writers, including the Active Directory writer, to prepare for writing data for shadow copy creation. Once the data is ready for the backup process, the writer notifies Volume Shadow Copy Service coordinator, which, in turn, relays that information to the backup requestor. The requestor briefly halts Active Directory I/O writes to disk for the few seconds it takes the provider to create the single point-in-time shadow copies of the three volumes.

Once a shadow copy of one or more volumes is made, Volume Shadow Copy Service can be instructed to break the connection between the original and the shadow copy. The shadow copy is now read-only, and the original data continues in production. At this point, the shadow copy is no longer associated with a particular server; it merely resides on the storage array until a need arises.

“Transport” through LUN Masking and Unmasking

In a SAN configuration, unlike with direct attached storage, actual physical transport of data from one server to another is unnecessary—the storage has been uncoupled from a specific server machine and is stored on an array where it can be accessed by multiple servers.

Although access to the storage pool is shared, each server can only access the specific LUNs assigned to it, since two servers cannot both write to the same volume without causing data corruption. But using the hardware provider on the SAN, a point-in-time shadow copy can be virtually “transported” to another server for use. This is done through the process of masking and unmasking through the Virtual Disk Service DISKRAID utility.

The failed LUNs are taken offline using the DISKRAID mask command. The backed-up shadow copy LUNs are then unmasked, converted from read-only status to read/write status, and then mounted for use on the failed server (which much be rebooted to return to production).

A generalized example of shadow copy creation and transport between two servers is shown in Figure 2. A single point-in-time shadow copy is made of the three volumes assigned to Server 1. This shadow copy set can be accessed by Server 2 through the process of first unmasking, then mounting the LUNs. The complete process is virtual “transport.”

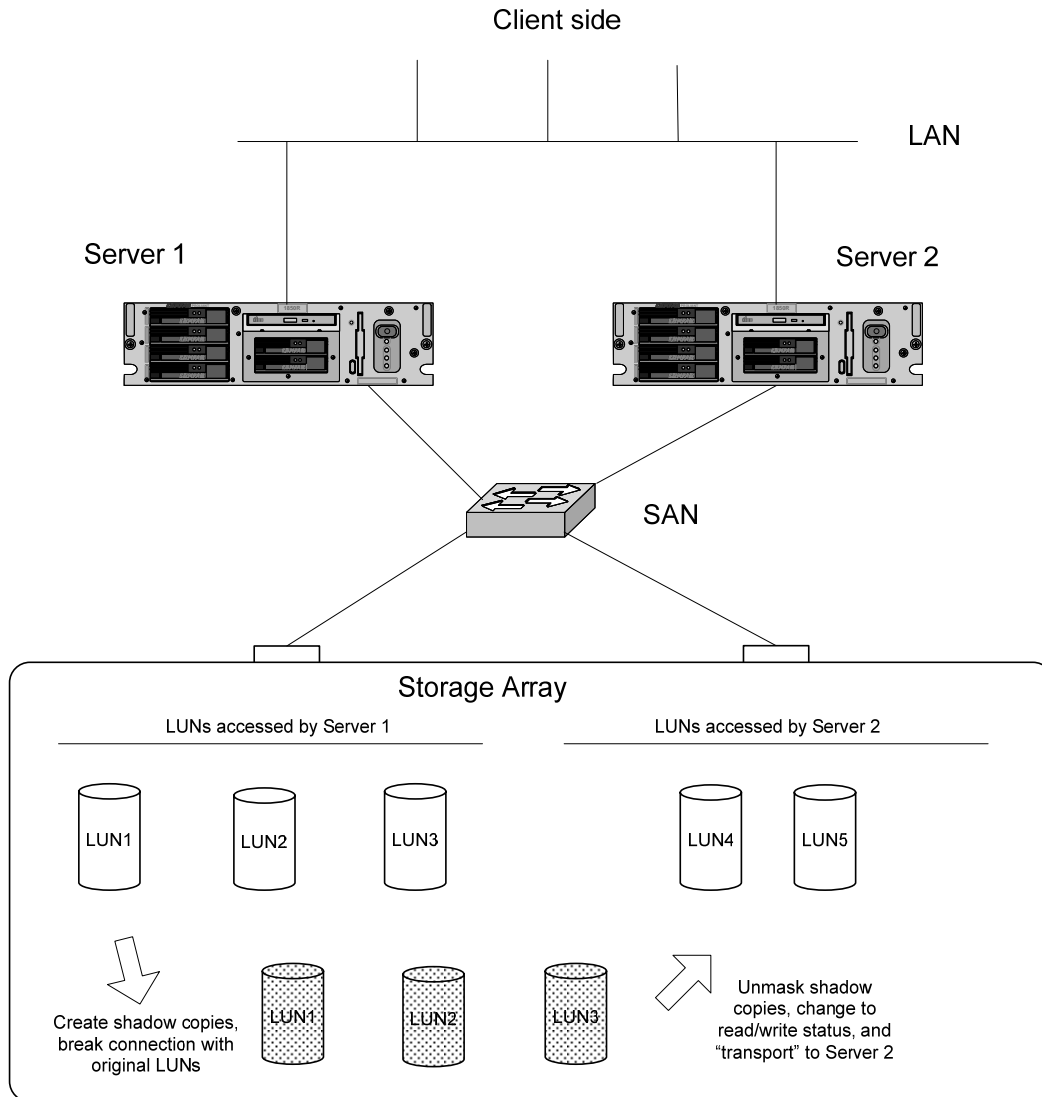


Figure 2. Shadow Copy Creation and Transport Between Two Servers

Note that Figure 2 is a general example of moving LUNs between two servers. It does not indicate that you can use a backup of one domain controller to restore another.

Boot from SAN

Active Directory is backed up as part of System State. This System State includes the Active Directory database and log files, as well as the registry, system boot files, COM+ registration database, and Sysvol. These data volumes cannot be broken; they must be handled as a set.

Windows requires a unique dedicated disk from which to boot the operating system. Normally an Active Directory server boots its operating system from an attached disk. However, in this scenario, because the Active Directory database and logs are stored on the SAN (which is critical for leveraging the hardware provider's transport capabilities that enable the fast recovery scenario to work), the operating system must also be stored on the SAN, thus keeping the System State intact.

Fast Recovery Demonstration

This section provides details regarding results of the demonstration and the hardware, software, and Windows Server 2003 configurations used in the Microsoft test labs to demonstrate fast recovery in an Active Directory environment.

Summary of Results

The hardware and software configurations used in the demonstration of fast recovery are described in this section. Table 1 outlines the steps to Active Directory recovery with and without the new capabilities of Windows Server 2003. In the demonstration configuration, Active Directory contained 20 million computer, user and contact objects in the ratio of 2:2:1, for a database size of 20 GB.

Table 1. Comparison of Fast Recovery in Windows Server 2003 and Previous OS Recovery Times

Steps to Restore Data			
Server 2000, NT	Time	Server 2003	Time
1) Analyze failure to determine if server can be recovered.	30-90 minutes	N/A	N/A
2) If unable to recover server, save corrupted data using <code>xcopy</code> or <code>robocopy</code> .	Minutes to hours, depending on amount of data	1) Use LUN masking to hide corrupted data (T_2); save for later analysis.	seconds
3) Retrieve tapes from offsite vault	Minutes to hours	N/A	N/A
4) Restore volumes from backup tape.	Minutes to hours	2) Using LUN unmasking, recover shadow copy volumes backed up at T_1 .	seconds
5) Reboot Active Directory Server	2 minutes	3) Reboot Active Directory Server (change HBA boot LUN).	2 minutes
6) Resynchronize with redundant machine.	Time between failure and restore long; can be significant data divergence	4) Resynchronize	Time between failure and restore minimal; limited data divergence
7) Resume production.	May be hours before production resumed	5) Resume production	Can return to full operations within 5 minutes of failure
8) No preventative action possible if corrupted data overwritten in step 3.		6) Analyze cause of failure; take preventative action	

Streamlined Recovery Management

In the past, if the system administrator wished to attempt to determine the cause of server failure, it was necessary to spend time, while the system was down and users were impacted, to attempt to analyze the problem. If the problem could not be identified, the administrator's only alternative was to restore data from tape, thus overwriting the corrupted data volumes and losing both the

ability to determine the source of the problem and the ability to take preventative action. With LUN masking, the corrupt data is not lost, but can be unmasked later to a secondary machine and analyzed at leisure to determine the cause of failure.

Faster Time to Restore

By using Windows Server 2003 connected to a storage area network, recovery time after Active Directory server failure is dramatically shortened. While resynchronization times are data dependent in both scenarios, restore times are dramatically decreased when using shadow copy restore. Restores from tape that previously took hours (or even days, depending on the size of the database) now take only minutes. Instead, shadow copies of the corrupt volumes can be accessed directly from the SAN, unmasked and made available to the failed server, which can, itself, be rebooted from the SAN. Rapid recovery minimizes the period of time in which changes to the data on the functioning server can occur, thus reducing resynchronization time.

Demonstration Configuration

Figure 3 shows the configuration used in the fast recovery demonstration.

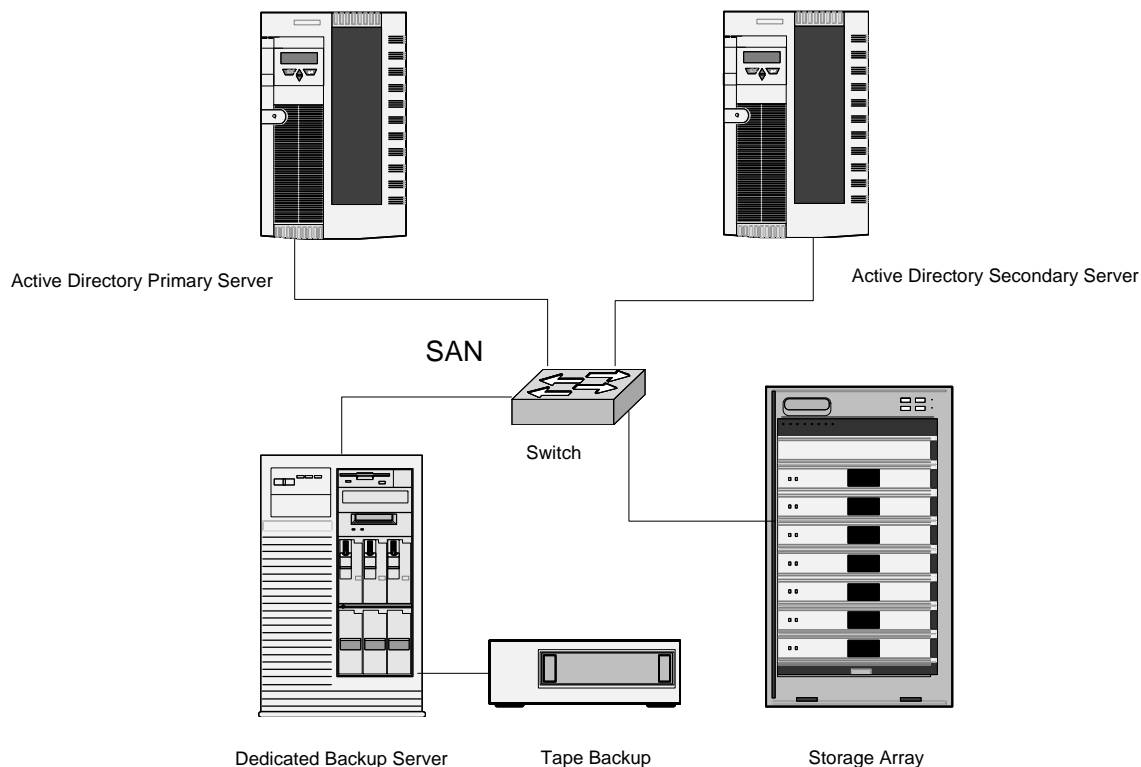


Figure 3. Test Hardware Configuration

The following components made up the test configuration of the storage area network depicted in Figure 3. Table 2 lists the specific hardware and software components.

Servers

- Two Active Directory servers (peer domain controllers; data is replicated between the two).
- A dedicated backup server.

Storage

- A tape backup system attached to the backup server.
- A storage disk array, with system state (operating system) data stored on volumes C:, Active Directory database and Sysvol on D:, and the Active Directory logs on E:.

Interconnects

- Fibre Channel switch to connect devices.
- Fibre Channel cables (multi-mode fiber).

Table 2 lists the hardware and software components used in the demonstration configuration.

Table 2. Hardware and Software Configurations

System	Hardware	Software
Active Directory Server 1 ("StorServ7"): Domain Controller 1	Compaq Proliant DL 320 single processor 512 MB RAM NO internal drive	Windows Server 2003, Enterprise Edition
Active Directory Server 2 ("ESD demo06"): Domain Controller 2	HP Proliant DL320 G2 Single processor Pentium 4 2.2 GHz 640 MB RAM NO internal drive	Windows Server 2003, Enterprise Edition
Dedicated Backup Server ("StorServ8")	HP LT 6000 2 processors XEON 2 GB RAM 32 GB disk 2 SCSI 18GB drive	Windows Server 2003, Enterprise Edition CommVault Galaxy v. 7.0
Tape drives and library	ADIC scalar 1000 4 LTO tape drives	N/A
Storage Array	HP VA-7400 45 disks 73 gigabyte drives total 3 terabytes info	Active Directory Volumes (Server 1): C: (LUN 1) 25 GB –contains operating system (with system/ boot volume) D: (LUN 2) 100 GB—contains Active Directory databases and Sysvol E: (LUN 3) 20 GB—contains Active Directory logs Active Directory Volumes (Server 2): C: (LUN 60) 25 GB –contains operating system/boot volume D: (LUN 61) 100 GB—contains Active Directory databases and Sysvol E: (LUN 62) 20 GB—contains Active Directory logs

Switch	QLogic 2 GB 16 port fibre switch	SAN software to manage SAN fabric
--------	--	-----------------------------------

Steps to Enable Fast Recovery

The system administrator must take a number of steps, both before and after an Active Directory server failure, to ensure successful fast recovery.

Prior to System Failure

The following steps must be taken to prepare for Active Directory server failure.

Initial System Setup (T₀)

For this Active Directory fast recovery scenario to work, three servers must be set up: two servers targeted for promotion to domain controllers, and a dedicated backup server. In the test scenario, Windows Server 2003, Enterprise Edition was installed on each domain controller server, using "Boot from SAN" guidelines per storage array vendor guidelines. Additionally, all three servers were configured with appropriate hardware and software to allow Volume Shadow Copy Service and Virtual Disk Service to function.

Domain Controller 1

1. Install Virtual Disk Service HW provider from HP for storage array
2. Install Volume Shadow Copy Service HW provider from HP for storage array
3. Promote server to domain controller
4. Install requestor. In this case, the CommVault Shadow Explorer was used.
5. Set the backup options by using the Shadow Explorer GUI, tools/options menu, as shown in Figure 4. Full backup and transport are allowed.

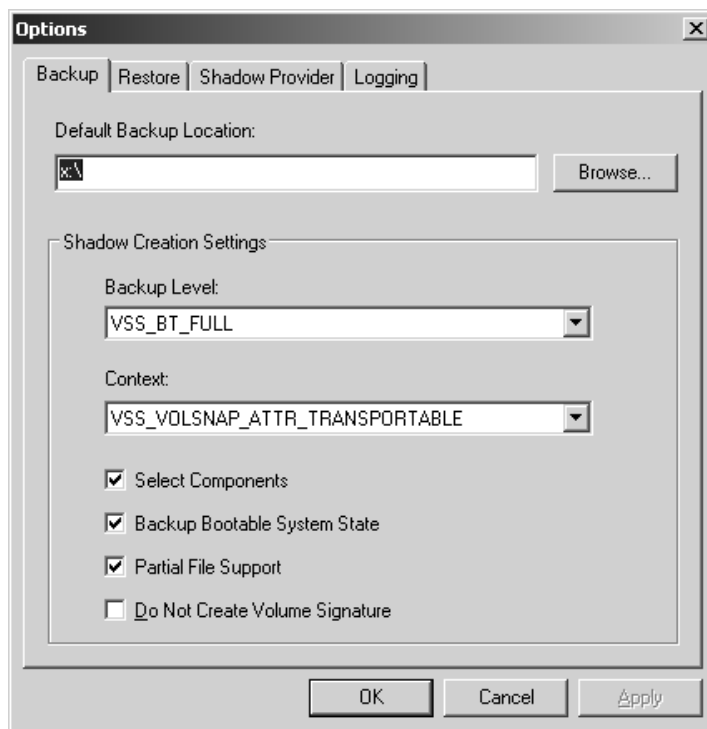


Figure 4. Screen Shot of Backup Options

Domain Controller 2

1. Promote to domain controller

Backup server

1. Install Virtual Disk Service HW provider from HP
2. Install Volume Shadow Copy Service HW provider from HP. See Figure 5.
3. Install CommVault Shadow Explorer. This part of the backup application makes the shadow copy.
4. Install CommVault Galaxy v 7.0 (this part of the backup application imports the shadow copy to the second machine)

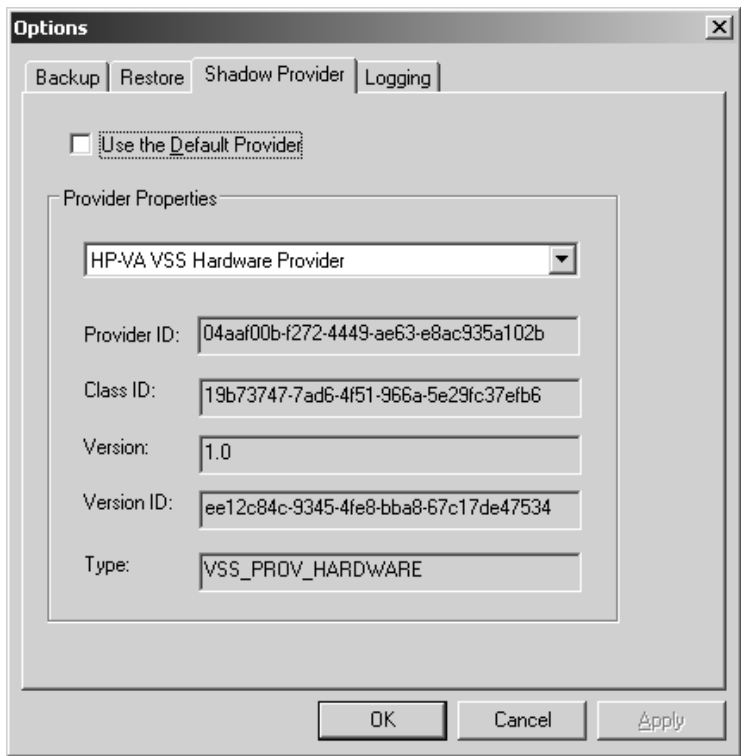


Figure 5. Screen Shot of HW Provider Information for Making Shadow Copies

Backup (T₁)

Domain Controller 1

1. Create shadow copy of System State (volumes C:, D:, E:) using Shadow Explorer requestor application with Volume Shadow Copy Service, as shown in Figure 6 The HW snapshots are created and held in the storage array.

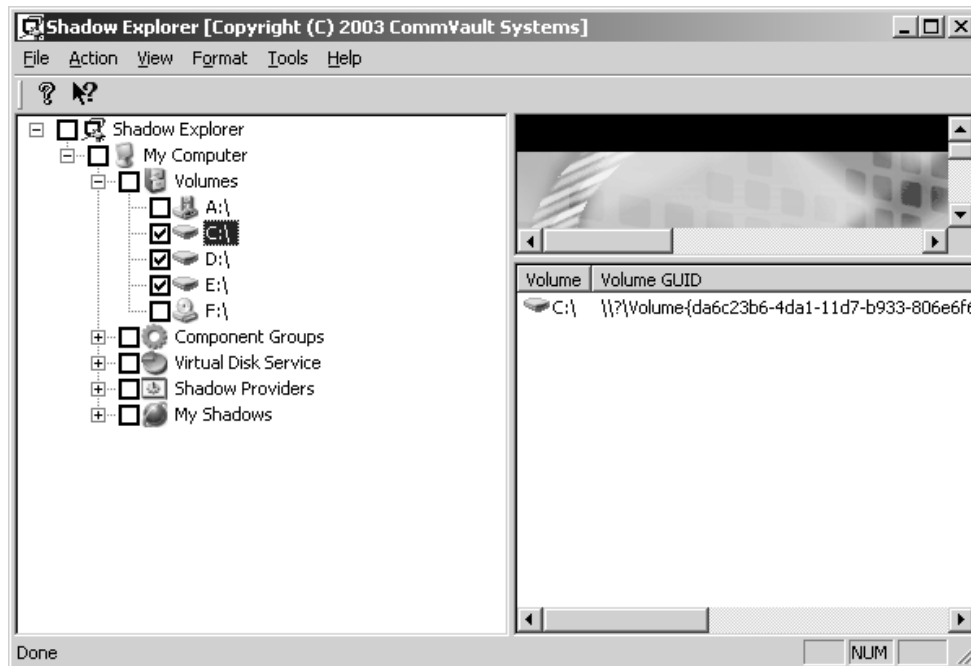


Figure 6. Screen shot of Shadow Explorer shadow copy creation

Backup Server

1. Import shadow copies of volumes C:, D:, E: into backup server (using Shadow Explorer GUI).
2. Run backup application to backup shadow copy volumes to tape drives.
3. Send tapes to disaster recovery site/cold vault for archiving.

Having accomplished these steps, system failure can now be dealt with rapidly. For the purposes of this demonstration scenario, system failure was simulated by masking the operating system volume (LUN 1) in the storage array such that Domain Controller 1 no longer has access. This was done as follows:

```
VDS> diskraid
DISKRAID> select sub 0
DISKRAID> select lun 1
DISKRAID> unmask lun none
```

The unmask lun none command ensures that the LUN is not accessible by any host. The process of selecting the boot LUN (LUN 1) and taking it offline simulates a hard drive crash resulting in a blue screen of the domain controller. The Active Directory workload is shifted over to Domain Controller 2.

Post System Failure

It is not necessary to take time to determine the root cause(s) to the problem at this stage. The system administrator merely protects the corrupted data for later analysis (by masking off the LUNs), then moves immediately to data restoration.

Note that successful recovery depends upon restoring the operating system and the Active Directory volume shadow copies as a complete set.

Restore Data (T₃)

Backup Server

1. Break shadow copies Shadow Explorer requestor application with Volume Shadow Copy Service
This action results in the deletion of Volume Shadow Copy Service database entries, which are specific to backup server, but not the deletion of the shadow copy LUNs.
2. Use Shadow Explorer to clear read-only volume settings.
These volumes are now just normal data volumes rather than shadow copies.

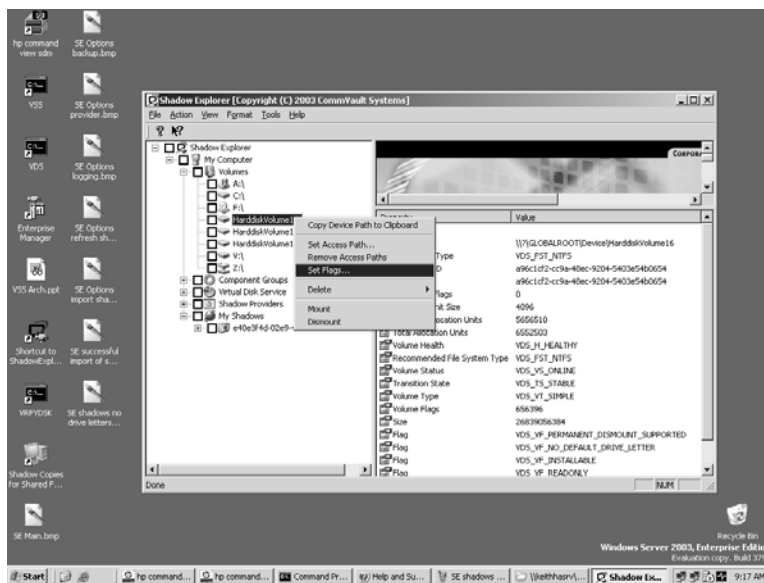


Figure 7. Screen Shot of Set Flags Option

3. Mask "failed" LUNs (1, 2 and 3) of Domain Controller 1, so that they are rendered inaccessible.
DISKRAID> unmask lun none
4. Mask LUNS surfaced on backup server to Domain Controller 1.
Note: Use the World Wide Name (wwn) identifier to determine which LUNs are the shadow copies for Domain Controller 1.
DISKRAID> select lun 6
DISKRAID> unmask lun wwn=10000000c92f203a
DISKRAID> select lun 7
DISKRAID> unmask lun wwn=10000000c92f203a
DISKRAID> select lun 9
DISKRAID> unmask lun wwn=10000000c92f203a
DISKRAID> exit

Domain Controller 1 (Boot from SAN)

1. Turn power on.
2. Enter Emulex HBA BIOS. **Alt E**.
3. Change BOOT LUN from "failed" LUN to "good" operating system LUN from previous point in time.
 - Set boot device. Select **1**.
 - Change existing boot setting. Select **01**.
 - Enter HEX# of LUN from which to boot. Enter **06**.
 - Boot 06 LUN by means of Disk ID (DID). Select **01**.

4. Reboot.

Resynchronize Data (T₄)

After Domain Controller 1 boots up, it performs a “hard” recovery of the Active Directory database, which includes replaying the logs, and synchronizes with Domain Controller 2 through regular Active Directory replication.

Return to Production (T₅)

The primary domain controller has now been returned to production, and workload has rapidly been restored to full capacity. The cause of the system failure can now be investigated at leisure, without impacting business operations. Having determined the cause of corruption, the system administrator can take preventative measures to help ensure that the problem is not repeated.

Conclusion

Fast restores using Volume Shadow Copy Service and Virtual Disk Service:

- Significantly reduce the recovery time of a failed Active Directory server on a storage area network.
- Streamline the process of managing recovery.
- Allow the system administrator to analyze root causes of failure without impacting the production environment.

These combined benefits enable the company to realize high data availability and robust data protection for Active Directory environments, while also allowing the system administrator to improve procedures for protecting data assets.

Related Resources

For additional benefits of using Volume Shadow Copy Service and Virtual Disk Service and more information about how they work, see “Storage Management using Windows Virtual Disk Service and Volume Shadow Copy Service,” on the Windows Powered NAS - White Papers Web page at <http://www.microsoft.com/windows/storage/productinformation/whitepapers>.



This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2003 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Windows, Windows NT, Windows 2000, Windows 2000 Server, and Windows Server 2003 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.