



**iStor Networks, Inc.™**

***Microsoft Windows Shadow Copies  
on the GigaStorATX***

**White Paper by  
David Cohen, iStor Networks Inc.**

**Revision .01**

June 28, 2006

**Abstract**

This paper outlines the use of Microsoft Windows Shadow Copies for administrators of the GigaStorATX.

<b>1. INTRODUCTION .....</b>	<b>4</b>
1.1. WHAT IS A SHADOW COPY? .....	4
1.2. BACKGROUND .....	4
1.3. DEFINITIONS .....	6
<b>2. USING THE VOLUME SHADOW COPIES FOR SHARED FOLDERS .....</b>	<b>7</b>
2.1. OVERVIEW.....	7
2.2. GIGASTORATX SETUP.....	8
2.3. MICROSOFT WINDOWS STORAGE SERVER 2003 R2 SETUP.....	9
2.4. CLIENT APPLICATION SETUP .....	12
<b>3. CONCLUSION .....</b>	<b>14</b>

© 2006 iStor Networks, Inc. All Rights Reserved

iStor Networks, Inc. makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. iStor Networks, Inc. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of iStor Networks, Inc.

The information is provided "as is" without warranty of any kind and is subject to change without notice. The only warranties for iStor 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. iStor shall not be liable for technical or editorial errors or omissions contained herein.

Copyright © 2006 iStor Networks, Inc.™

## Trademarks

Microsoft Windows is a U.S. registered trademarks of Microsoft Corporation.

All other brand or product names are or may be trademarks or service marks, and are used to identify products or services, of their respective owners.

iStor Networks, Inc.  
7585 Irvine Center Drive  
Suite 250  
Irvine, CA 92618  
[www.istor.com](http://www.istor.com)

## 1. Introduction

### 1.1. What is a Shadow Copy?

A Shadow Copy is a point-in-time copy of data used by an application. The purpose of a shadow copy is to allow the restore of data back to the particular point in time that the shadow copy represents. The shadow copy may include registry entries, object properties, files, directories, or volumes. The data included in the shadow copy is defined by the application that uses it. The goal of Microsoft Volume Shadow Copy Service is to insure that a shadow copy is always in a state that the data is useable and complete. Minimally, VSS requires that the data be “Crash Consistent” meaning that it is in a state similar to what would happen to the data if the computer lost power while an application was using the data.

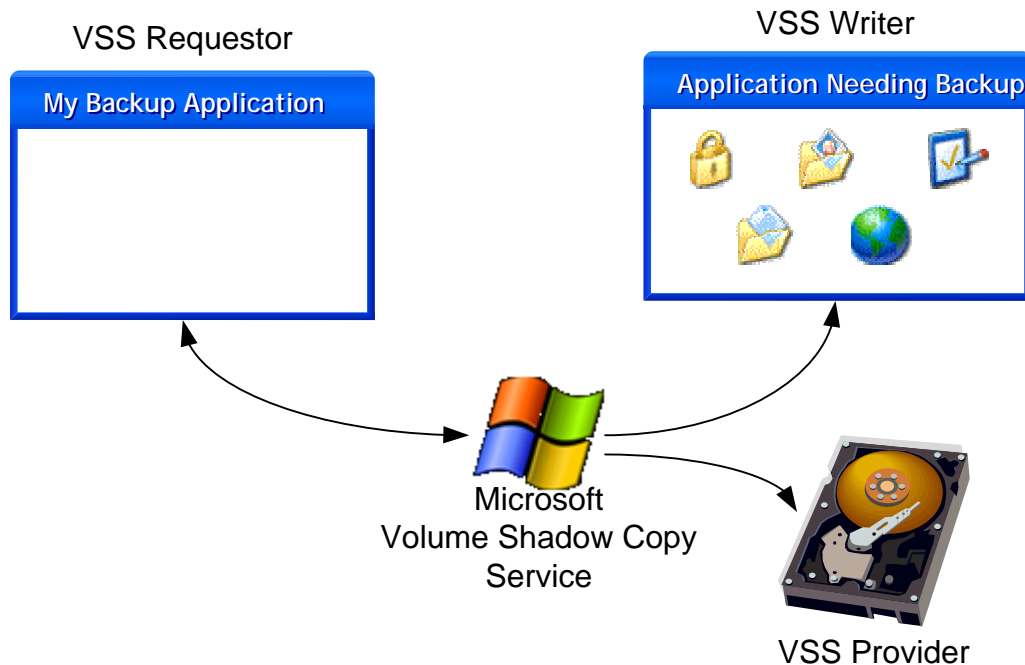
Shadow copies should not be confused with snapshots or mirrors. The actual implementation of the shadow copy changes based on the underlying data and is transparent to the user. Shadow copies are important to users because they allow users to:

- Recover files that were accidentally deleted.
- Undo changes in files that were accidentally overwritten.
- Compare changes written to files while working on the files.

### 1.2. Background

Shadow Copies and their management are a standard feature of Microsoft Windows Storage Server 2003 R2, and require no special GigaStorATX or iStor configuration. There is however a recommended configuration and best use of the GigaStorATX for shadow copy enabled volumes and administrators on SANs that use the GigaStorATX as their iSCSI target can benefit from an understanding of how to use the Microsoft Volume Shadow Copy Service. The purpose of this document is to provide GigaStorATX administrators an outline of the use of the Microsoft Volume Shadow Copy Service.

Using Microsoft Volume Shadow Copy Service, backup technology in the Microsoft Windows operating system has evolved from a simple file copy operation to a full copy management system. In the Microsoft Windows operating system today, users are encouraged to think of their data in terms of how they use it rather than where the data is physically stored. Consider a generic application that has multiple configuration files, some registry entries, and perhaps a database spread over several files in a data directory. Prior to VSS, the backup of this application would require that the configuration files, the registry entries, and the data directory all be included in the backup. This implies that the backup administrator has knowledge of how every application in the organization persists its data and where that data is located. Otherwise, the backup may or may not be complete. Additionally, if the required components are copied while the application is running, there may be cached data that has not yet been written to disk making the backup unusable. VSS solves these problems by coordinating the backup operation between the backup application, the application that owns the data, and software responsible for doing the actual copy.



**Figure 1 - The Shadow Copy Process**

To initiate a backup, a backup application (known in the VSS world as a “VSS Requestor”) tells the VSS Service that it would like to backup a specific application. The VSS Service finds that application (known in the VSS world as a “VSS Writer”) if it is currently running, and negotiates between the writer and the requestor to define exactly what data needs to be backed up and where that data is located. Based on the location of the data, VSS finds and loads software known as a “VSS Provider”. The VSS provider is software that accepts responsibility for performing the write for the copy of the data. Once all the pieces are in place and VSS knows what data is required for the backup, where that data is, and who will take responsibility for the process of performing the copy, the shadow copy process can really start. During the shadow copy process, VSS asks the writer to finalize any writing operations it may be performing and flush any data that it may have in memory to permanent storage. Once the writer completes writing, it notifies VSS and VSS asks the provider to copy the data that will be in the shadow copy. When the provider has completed copying, it notifies VSS that the operation is complete and VSS notifies the writer that it may resume normal operation. VSS finalizes the backup by creating a manifest of the details of shadow copy, cataloging the shadow copy in the VSS database, and notifying the backup application.

Microsoft Windows Storage Server 2003 R2 has included VSS requestor functionality in Disk Manager for creating shadow copies, and VSS requestor functionality in an add-in for Microsoft Windows Explorer for restoring shadow copies. The file system in Microsoft Windows Storage Server 2003 R2 acts as the VSS writer during shadow copy creation. The requestor in Disk Manager is simply called “Shadow Copies”, and the add-in for Microsoft Windows Explorer is called “Previous Versions”. The remaining sections of this white paper will discuss the use of both the “Shadow Copies” requestor and “Previous Versions” requestor.

## 1.3. Definitions

Term	Definition
administrator	An individual responsible for the creation and/or maintenance of network resources in an organization.
Application	A single software component used to perform a single or group of tasks. For example: Microsoft Exchange, Oracle, or Word Perfect.
backup	A version of data saved in case the original data is lost or corrupted.
Computer Manager	The application in Microsoft Windows used to manage computer or server systems. Also known as MMC.
configuration file	A file that is used to store configuration settings.
Crash Consistent Data	Data in a state identical to a computer losing power while the data is in use on that computer.
data	A set of information used by a computer.
Disk Manager	The MMC Snap-In that is used to manage disks in a Microsoft Windows system.
end user	A person that uses a computer.
GigaStorATX	The first in the family of iSCSI storage targets created by iStor Networks, Inc.
Host Microsoft Windows Storage Server 2003 R2	A computer running Microsoft Windows Storage Server 2003 R2 and an iSCSI initiator connected to an iSCSI target.
initiator	Software or hardware used to connect to an iSCSI target.
iSCSI Target	The network entity used by an iSCSI initiator to gain access to a storage volume.
MMC Snap-In	An application created to be used inside the Microsoft Windows Computer Manager.
Microsoft Windows Storage Server 2003 R2	The latest version of Microsoft Windows Server that supports advanced storage technology.
Mirror	A volume with an exact complete copy of its data to be used as a redundant data set in the case of drive failure.
Original volume	A volume that has shadow copies taken of it.
Point-in-time copy	A copy of data at a particular date and time.
Previous Versions	The client software distributed as a part of the VSS file system client.
Registry entry	A configuration setting saved in the Microsoft Windows

	Registry database.
SAN	Storage Area Network.
Shadow Copy	A backup of data saved by Microsoft Volume Shadow Copy Service.
Shadow Copy Set	A group of shadow copies that have the same Shadow Copy Set Id so that they can be backed up and restored together as a single unit.
Shared folder	A directory on a file server that allows multiple users to read, write, or read/write to it.
SMS	System Management Services – A software application that is responsible for the deployment, upgrade, and licensing of applications across a Microsoft Windows network.
Snapshot	A volume that points to blocks as they were at a specific point in time.
Volume Shadow Copy Service	A Microsoft Service for Microsoft Windows Storage Server that supports the shadow copy functionality.
VSS	Microsoft Volume Shadow Copy Service.
VSS Provider	Software that is responsible for the copy process during shadow copy creation.
VSS Requester	An application that manages shadow copies.
VSS Writer	An application that uses the data to be backed up by shadow copies.

**Table 1 - Definitions**

## 2. Using the Volume Shadow Copies for Shared Folders

### 2.1. Overview

Shared files and directories located on file servers running Microsoft Windows Storage Server 2003 R2 can be automatically backed up for easy restoral by users.

To create the shadow copies, the administrator of the file server first selects volume to shadow copy. All users with access privileges to the files and folders on the original volume will have access to the shadow copies of those files and folders. The next decision for the administrator is how often the volume should be shadow copied. The schedule can be entered in the “Shadow Copies” tab of the volume “Properties” dialog. Once the shadow copy schedule is established, the administrator must select a location for the shadow copies to be stored. If the shadow copies are to be stored on the same volume as the original folders and volumes, a minimum of 300 megabytes will be required. GigaStorATX owners should create a separate volume to act as a repository for the shadow copies. The host Microsoft Windows Storage Server 2003 R2 will require access to both volumes, but access to the volume containing the shadow copies can be restricted from users who have access to the original volume.

The shadow copies will automatically be created and rotated. They will be created based on the schedule defined by the administrator, and they will be rotated when the location reserved for shadow copies is full. There is currently

a limit of 64 shadow copies per volume, and therefore shadow copies beyond the 64<sup>th</sup> will be rotated. When shadow copies are rotated, the oldest is deleted and a new one takes its place.

To use shadow copies, a user simply needs to right mouse click on a shared file or directory that is located on a Microsoft Windows Storage Server 2003 R2 file server and has shadow copies available. From the right mouse click menu, the Properties dialog is opened. There will be an additional tab in the Properties dialog entitled “Previous Versions”. On the Previous Versions tab is a list of all shadow copies available listed by time and date. The user may select a shadow copy to restore, copy, or view.

## 2.2. GigaStorATX Setup

The GigaStorATX requires very little setup to support the Microsoft Volume Shadow Copy Service. iStor recommends that for every original volume that will have shadow copies, an additional volume be created to store the shadow copies. It is also recommended that the volume used to store the shadow copies be a Parity volume no matter what the composition of the original volume. From the GigaStor Management Console application that comes with the GigaStorATX the steps to setup the GigaStorATX are:

1. Create the original volume. If the original volume already exists, or is not located on the GigaStorATX this step may be skipped.
2. Create a parity volume to store the shadow copies. Microsoft recommends that space equal to at least 20% of the size of the original volume be allocated for shadow copies. iStor recommends creating a volume to store the shadow copies up to the same size of the original. Whatever the size allocated for the volume to hold the shadow copies, the GigaStorATX offers the opportunity to grow the volume at a later date if more space is required. The parity volume should have a stripe width big enough to minimize the impact of rebuild operations, and at the same time leave available enough drives in the GigaStorATX so that rebuild operations can take place as needed in the case of drive failure.
3. Create an iSCSI access path for the volumes. The initiator for the host Microsoft Windows Storage Server 2003 R2 must be entered, either a shared port for both volumes or separate ports for the volumes must be created, and either a single target for both volumes or separate targets for the volumes must be created.

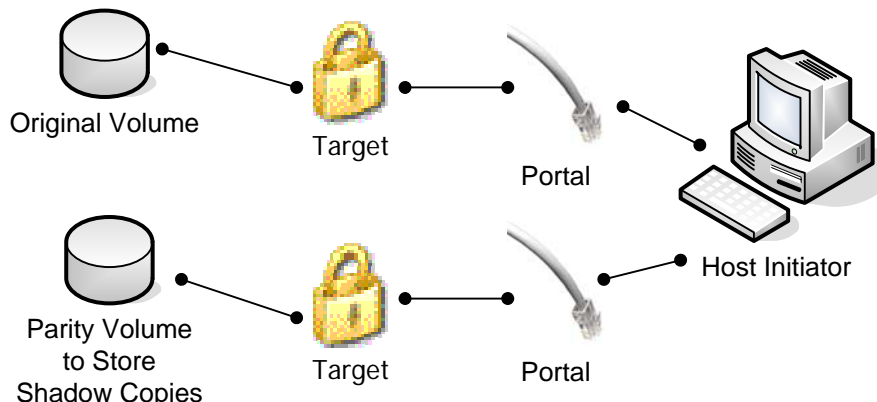
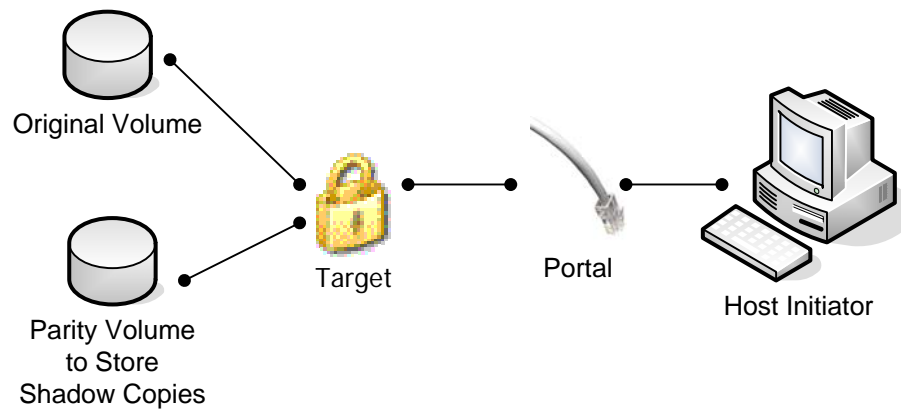


Figure 2 - Separate iSCSI Access Paths to GigaStorATX Volumes

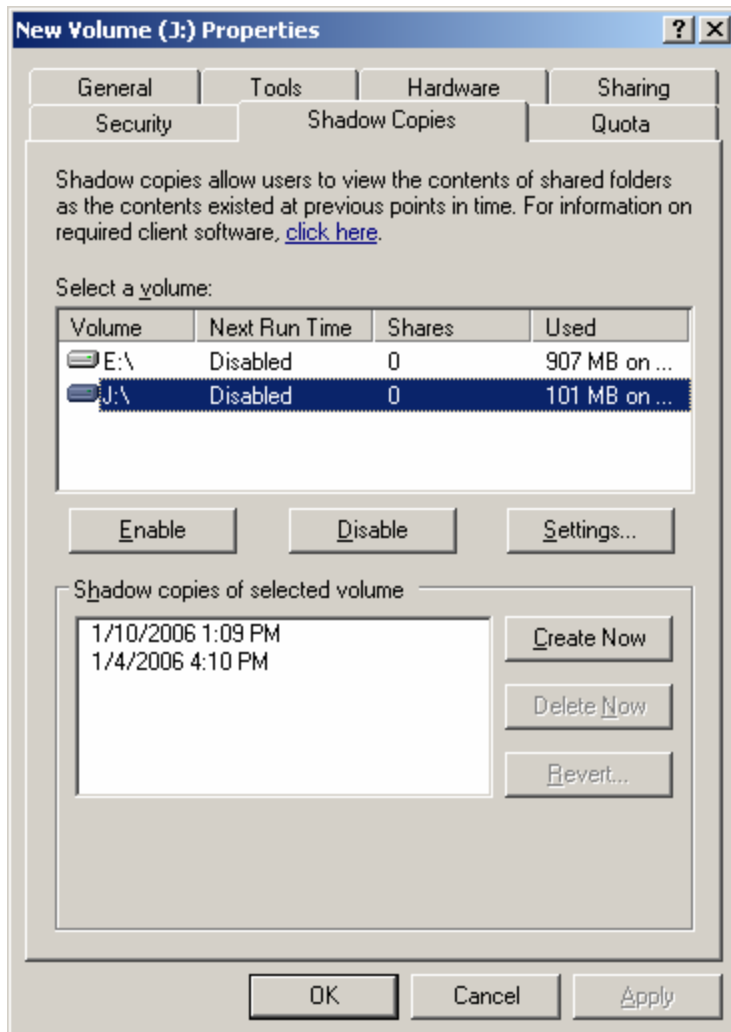


**Figure 3 - Alternative Shared iSCSI Access Path to GigaStorATX Volumes**

## 2.3. Microsoft Windows Storage Server 2003 R2 Setup

Once the GigaStorATX grants access to the volumes, the file server may log in and configure the Volume Shadow Copy Service. The configuration for Volume Shadow Copy Service can be found by opening the Computer Manager in the Administrative Tools section of the Microsoft Windows Start menu. In the explorer bar in the Computer Manager main window Disk Manager is identified as “Disk Management”. It is important to understand that GigaStorATX volumes appear as “disks” in the Disk Manager. The steps to configure the Microsoft Windows Storage Server 2003 R2 file server are:

1. Log in to the target(s) from the host initiator and initialize the drives. From the Management Console select the Disk Manager plug-in and initialize the drives that access the volumes on the GigaStorATX. If the drive to be used as the original volume is already initialized, this step may be skipped for that drive.
2. Format and map a drive letter to the original volume as well as the volume to be used to save the shadow copies. If the drive for the original volume already has been formatted and has a drive letter, this step may be skipped for that drive.
3. From the right-mouse-click pop-up menu of the original volume disk select “Properties”. When the Properties dialog appears, select the “Shadow Copies” tab.



**Figure 4 - Shadow Copies Tab of Disk Properties Dialog**

4. Click the “Settings” button to to select the disk to store the shadow copies as the location for the shadow copies to be stored. Increase the amount of space on the volume to be used to store shadow copies to the entire volume. Using the GigaStorATX, the volume that is to hold the shadow copies should be used for the shadow copies *only*.

# Microsoft Windows Shadow Copies on the GigaStorATX

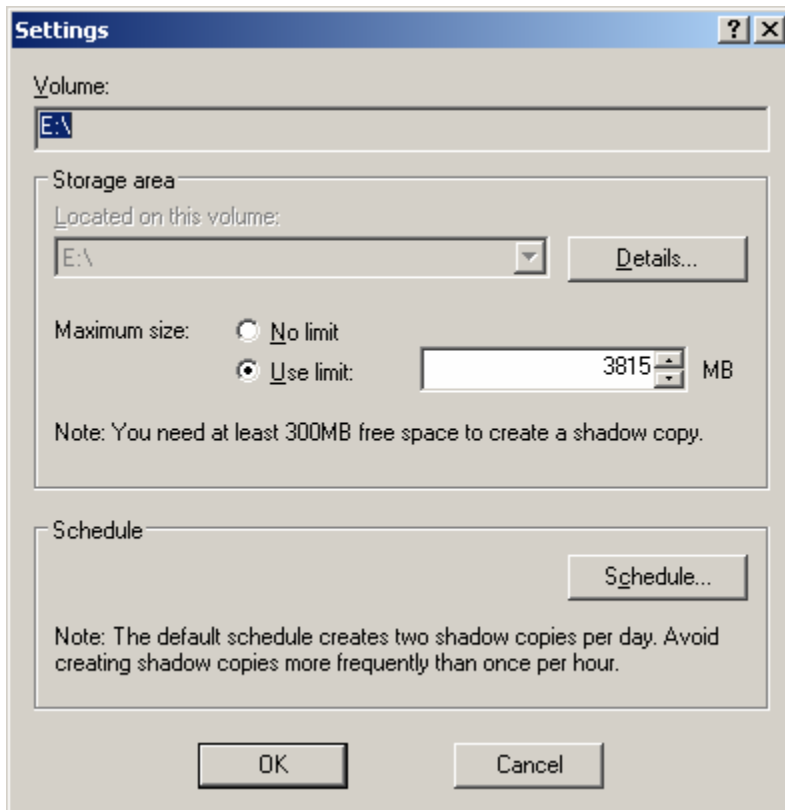
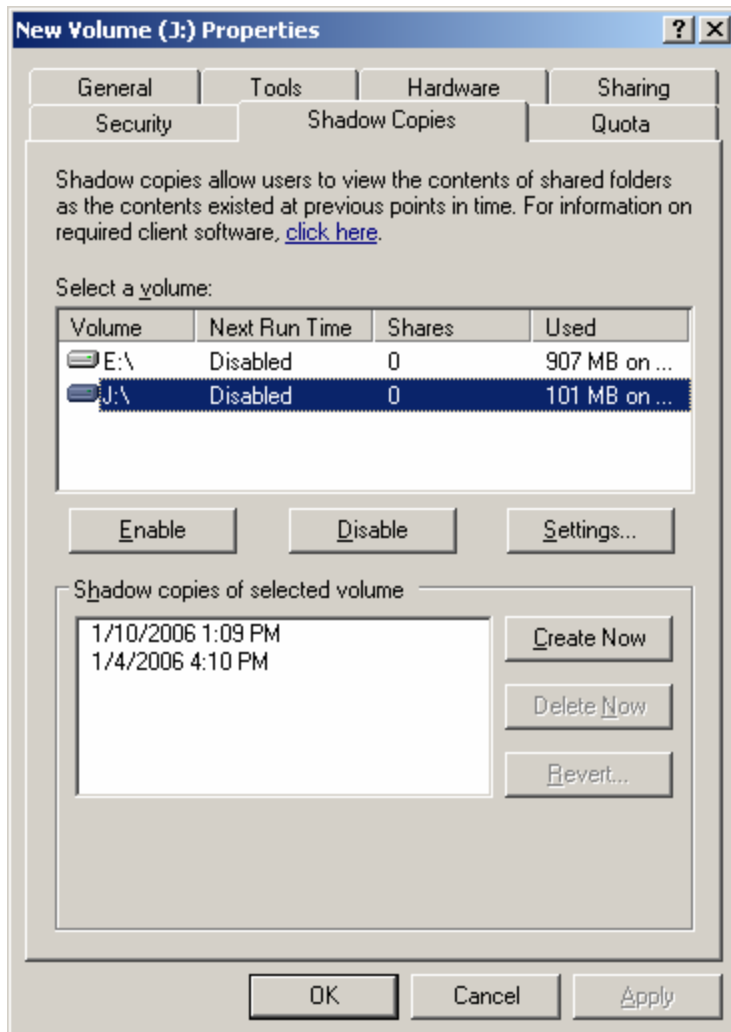


Figure 5 - Shadow Copies Settings Dialog

5. Click the “Schedule” button to establish the schedule for creating shadow copies.



**Figure 6 - Shadow Copies Schedule Dialog**

6. Click the “Create Now” button to create the first baseline shadow copy of the volume.

## 2.4. Client Application Setup

The client application available for the Volume Shadow Copy Service is used to retrieve past versions of a file, directory, or volume. It does not create shadow copies – that is the job of the file server. The client runs on Microsoft Windows XP, Microsoft Windows 2000, and Microsoft Windows 2003. It is not necessarily installed. Microsoft recommends that the client application be available on the network placed on a shared resource for download and installation, or better yet deployed by System Management Service. The client installer file name is ShadowCopyClient.msi. The client is most often referred to as “Past Versions”, and is available through any Microsoft Windows Explorer right click menu.

## Microsoft Windows Shadow Copies on the GigaStorATX

The steps to gain access to a past version (shadow copy) of a file or directory are:

1. Install the client software on the local client computer by running ShadowCopyClient.msi.
2. Right mouse click on the file or directory of interest. From the pop-up-menu select “Properties”. From the Properties dialog select the “Previous Versions” tab.

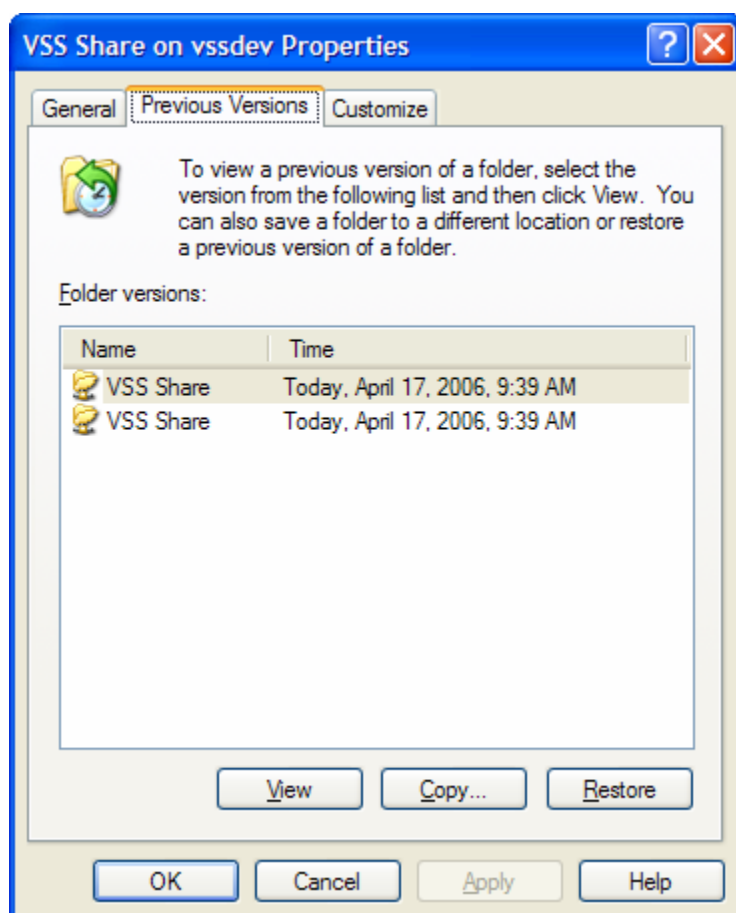


Figure 7 - Previous Versions Tab of the File Properties Dialog

3. On the Previous Versions tab a list of available shadow copies will be displayed sorted by time and date.
  - To restore the file to the time and date listed, select the “Restore” button.
  - To open the file as it was on the time and date listed, select the “View” button.
  - To compare the shadow copy to the original select the “Copy” button and copy the shadow to a new file name.

## 3. Conclusion

The GigaStorATX provides an excellent platform for the Microsoft Volume Shadow Copy Service because of the flexibility it provides in access path management, the ease of managing the relationship between original and shadow volumes, the ability to grow volumes holding shadow copies as needed, and the ability to restrict user access to the volume holding the shadow copies.

Microsoft has created an exceptionally useful and reliable model for the backup and restore of filesystem files. The VSS writer and requestor included in Microsoft Windows Storage Server 2003 R2 seamlessly integrate the concepts of backup and restore into the file system in a manner that is easy for users to learn.

The combination of the GigaStorATX and Microsoft Windows Storage Server 2004 R2 is a powerful tool for administrators of networks of any size.