Designing a Shadow Copy Strategy

7 out of 9 rated this helpful

Updated: March 28, 2003

Applies To: Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2

You can give users access to previous versions of files by enabling shadow copies, which provide point-in-time copies of files stored on file servers running Windows Server 2003. By enabling shadow copies, you can reduce the administrative burden of restoring previously backed up files for users who accidentally delete or overwrite important files. Shadow copies work for both open and closed files; therefore, shadow copies can be taken even when files are in use.

Shadow copies work by making a block-level copy of any changes that have occurred to files since the last shadow copy. Only the changes are copied, not the entire file. As a result, previous versions of files do not usually take up as much disk space as the current file, although the amount of disk space used for changes can vary depending on the application that changed the file. For example, some applications rewrite the entire file when a change is made, whereas other applications append changes to the existing file. If the entire file is rewritten to disk, the shadow copy contains the entire file. Therefore, consider the type of applications in your organization, as well as the frequency and number of updates, when you determine how much disk space to allocate for shadow copies.

Important

- Shadow copies do not eliminate the need to perform regular backups, nor do shadow copies protect you from media failure. In addition, shadow copies are not permanent. As new shadow copies are taken, old shadow copies are purged when the size of all shadow copies reaches a configurable maximum or when the number of shadow copies reaches 64, whichever is sooner. As a result, shadow copies might not be present for as long as users expect them to be. Be sure to consider user needs and expectations when you configure shadow copies.

Shadow copies are designed for volumes that store user data, such as home directories and My Documents folders that are redirected by using Group Policy, or other shared folders where users store data. Shadow copies work with compressed or encrypted files, and they retain whatever permissions were set on the files when the shadow copies were taken. For example, if a user is denied permission to read a file, that user would not be able to restore a previous version of the file, nor would the user be able to read the file after it has been restored.

Although shadow copies are taken for an entire volume, users must use shared folders to access shadow copies. Administrators on the local server must also specify the *servername**sharename* path to access shadow copies. If you or your users want to access a previous version of a file that does not reside in a shared folder, you must first share the folder.

Collecting Information to Design a Shadow Copy Strategy

When you design a shadow copy strategy, review the following topics. For an Excel spreadsheet to assist you

in documenting your shadow copy design decisions, see "Shadow Copy and Disk Quota Configuration Worksheet" (Sdcfsv_7.xls) on the *Windows Server 2003 Deployment Kit* companion CD (or see "DFS Configuration Worksheet" on the Web at http://www.microsoft.com/reskit).

Shadow copy support in client operating systems

Shadow copies can be accessed by computers running Windows Server 2003 and by computers running Windows XP Professional on which you have installed the Previous Versions Client pack (Twcli32.msi). This file is located in the Windows Server 2003 operating system in *windir*\system32\clients\twclient. You can install this file manually on clients or deploy the file by using the software distribution component of Group Policy. For more information about software distribution, see "Deploying a Managed Software Environment" in *Designing a Managed Environment* of this kit.

To access shadow copies from previous versions of Windows, including Windows 2000 and Windows XP Professional, you can download and install the Shadow Copy Client. For more information and to download the Shadow Copy Client, see the Shadow Copy Client Download link on the Web Resources page at http://www.microsoft.com/windows/reskits/webresources.

Note

- The Previous Versions Client and the Shadow Copy Client provide the same functionality, but the Shadow Copy Client can be installed on multiple operating systems, such as Windows 2000 and Windows XP Professional, whereas the Previous Versions Client can only be installed on Windows XP Professional.

If you have not yet deployed these operating systems or client packs on your clients, you can deploy a single computer (or as many as necessary) from which users can restore previous versions of files. You can also distribute the client pack on a case-by-case basis to users who request that files be restored.

Shadow copy support in server operating systems

Shadow copies are available only on file servers running Windows Server 2003.

Shadow copy support on server clusters

There are a number of important considerations for managing shadow copies on cluster storage. For more information about managing shadow copies on server clusters, see "Using Shadow Copies of Shared Folders in a server cluster" in Help and Support Center for Windows Server 2003.

File system requirements

Shadow copies are available only on NTFS volumes.

Recommended scenarios for using shadow copies

Shadow copies work best when the server stores user files such as documents, spreadsheets, and graphics files. Do not use shadow copies to provide access to previous versions of application or e-mail databases.

Amount of volume space to allocate to shadow copies

When you enable shadow copies on a volume, you can specify the maximum amount of volume space to be used for the shadow copies. The default limit is 10 percent of the source volume (the volume being copied).

Increase the limit for volumes where users frequently change files. Also, setting the limit too small causes the oldest shadow copies to be deleted frequently, which defeats the purpose of shadow copies and which will likely frustrate users. In fact, if the amount of changes is greater than the amount of space allocated to storing shadow copies, no shadow copy is created. Therefore, carefully consider the amount of disk space that you want to set aside for shadow copies, while keeping in mind user expectations for how many versions they want to be available. Your users might expect only a single shadow copy to be available, or they might expect three days' or three weeks' worth of shadow copies. The more shadow copies the users expect, the more storage you need to allocate for storing them.

Setting the limit too small can adversely affect other programs, such as the Backup program in Windows Server 2003 and other backup programs that support the Volume Shadow Copy service. During the backup process, these programs create temporary shadow copies for consistent backups. The temporary shadow copies count towards the volume space limit you specify for shadow copies. If the available volume space remaining in the limit is too small, the Volume Shadow Copy service can delete existing shadow copies to free up space for the temporary shadow copy. If there are no existing shadow copies, and the volume space limit cannot accommodate the temporary shadow copy, the backup might fail. For more information about the Volume Shadow Copy service, see the Storage Services link on the Web Resources page at http://www.microsoft.com/windows/reskits/webresources.

Important

- Regardless of the volume space that you allocate for shadow copies, you can have a maximum of 64 shadow copies for any volume. When the 65th shadow copy is taken, the oldest shadow copy is purged.

Frequency at which Windows Server 2003 creates shadow copies

By default, Windows Server 2003 creates shadow copies at 7:00 A.M. and at 12:00 noon Monday through Friday. However, you can change the schedule to better accommodate users. Keep in mind that the more shadow copies you create, the more disk space the shadow copies can consume, especially if files change frequently. When you determine the schedule, avoid scheduling shadow copies to occur more than once per hour.

Storing shadow copies on separate disks

You can dedicate a volume on separate disks for storing the shadow copies of another volume on the same file server. For example, if user files are stored on H:\, you might use another volume, such as S:\, to store the shadow copies. Using a separate volume on separate disks provides better performance, and it is recommended for heavily used file servers. If you plan to use a separate volume for the storage area (where the shadow copies are stored), be sure to change the maximum size to **No Limit** to reflect the space available on the storage area volume instead of the source volume (where the user files are stored).

Important

- If you plan to store the shadow copies on the same volume as the user files, note that a burst of disk I/O can cause all shadow copies to be deleted. If you cannot tolerate the sudden deletion of shadow copies, use a volume that will not be shadow copied, preferably on separate disks, for storing shadow copies.

File servers containing mounted drives

A mounted drive is a local volume attached to an empty folder (called a *mount point*) on an NTFS volume. If you enable shadow copies on a volume that contains mounted drives, the mounted drives are not included when shadow copies are taken. In addition, if you share a mounted drive and enable shadow copies on it, users cannot access the shadow copies if they traverse from the host volume (where the mount point is stored) to the mounted drive.

For example, assume you have the folder E:\Data\Users, and the Users folder is a mount point for F:\. You enable shadow copies on both E:\ and F:\, you share E:\Data as \\Server1\Data, and you share E:\Data\Users as \\Server1\Users. In this example, users can access previous versions of \\Server1\Data and \\Server1\Users but not \\Server1\Data\Users.

Defragmenting the volume where shadow copied files are stored

If you plan to defragment volumes on which shadow copies are enabled, it is recommended that you use a cluster (or allocation unit) size of 16 KB or larger. If you do not, the number of changes caused by the defragmentation process can cause shadow copies to be deleted faster than expected. Note, however, that NTFS compression is supported only if the cluster size is 4 KB or smaller.

Note

- To check the cluster size of a volume, use the **fsutil fsinfo ntfsinfo** command. If the volume contains data and you want to change the cluster size, you must back up the data on the volume, reformat it using the new cluster size, and then restore the data.

Converting basic disks to dynamic disks

If the volumes that contain the original files and the shadow copy storage area are on separate basic disks and you want to convert both of the disks to dynamic disks, you must follow these directions:

- **If the shadow copy storage area is not on the boot volume.** First dismount and take offline the volume that contains the original files. To do this, use Mountvol.exe with the /p parameter. Next, convert the disk that contains the storage area volume to a dynamic disk. After the conversion, you have 20 minutes to mount the volume that contains the original files and bring it online by using Mountvol.exe or the Disk Management snap-in; if you do not, you will lose the existing shadow copies. After you bring the volume that contains the original files back online, you can convert that disk to a dynamic disk.

- **If the shadow copy storage area is on the boot volume.** You can convert the disk that contains the storage area volume to a dynamic disk without having to dismount the volume that contains the original files. To complete the conversion, you must restart the computer twice. Next, convert the disk that contains the original files to a dynamic disk.

Important

- If the disk that contains the original files is converted to a dynamic disk first, the shadow copies are deleted when you convert the disk that contains the storage area volume to a dynamic disk.

Using DFS to provide access to volumes that contain shadow copies

You can create DFS link targets on volumes that contain shadow copies, and users can retrieve previous versions of files from the DFS link target, just as they can from a regular shared folder. However, if you use multiple link targets for a DFS link, each of those link targets can reside on a different volume with its own shadow copies. As a result, the previous versions of files can vary, depending on which link target the user last accesses to change the file.

Backing up shadow copies

Windows Server 2003 does not support backing up shadow copies. When you back up a volume, shadow copies are not backed up.

Using scripting to create shadow copies

To create shadow copies by using scripts, use Vssadmin.exe to create the shadow copies and, optionally, use Schtasks.exe to schedule the creation of shadow copies. For more information about using these command-line tools, see "Vssadmin" and "Schtasks" in Help and Support Center for Windows Server 2003.

For more information about shadow copies, see "Shadow Copies for Shared Folders" in Help and Support Center for Windows Server 2003.

Example: An Organization Designs a Shadow Copy Strategy

A large organization allows users to redirect their My Documents folders to a central file server. When a user accidentally deletes or overwrites a file and requests that the file be restored, the process requires between 1 day and 3 days and up to three escalations before the backup/restore group can restore a file. The organization determines that it costs approximately $300 for support and escalation costs plus lost productivity while the restoration takes place.

To decrease the cost associated with restoring files and to increase user satisfaction, the organization enables shadow copies on its file servers. During the pilot program, the organization determines that the default settings for the schedule and storage volume allow two weeks of previous versions. When a user contacts the support group to have a file restored, the support group provides a copy of the Previous Versions Client pack to the user. It takes the user approximately five minutes to install the software and another five minutes to restore the file. As a result, a user can restore a file in 10 minutes instead of 1 day to 3 days, and user satisfaction is greatly increased.

Did you find this helpful?　　◯ Yes　　　◯ No

Community Additions