Persistent Storage Manager™

PSM/SAK

Engineering and Product Marketing Documents

Documentation for OEM customers integrating PSM with the Microsoft SAK (Server Appliance Kit). Documentation includes; Installation Guide, User Guide, Product Overview, Specification Sheet, and Event Log Error Codes.

Additional information located at < www.cdp.com/library/PSM/tech/ >.

Information contained herein is believed to be accurate at the time of publication.

Persistent Storage Manager, PSM, Persistent True Image, PTI, OTM, Open Transaction Manager are Trademarks of Columbia Data Products. The entire document ©2002 Columbia Data Products, Inc.

Columbia Data Products, Inc.
Box 163088, Altamonte Springs, FL 32716
800/613-6288 – www.cdp.com

Persistent Storage Manager™ Patents Pending

T A B L E   O F   C O N T E N T S

I. Persistent Storage Manager™ Overview

1. Introduction

The most valuable commodity of the Information Age is data. An interruption in the flow of data from virus attacks, file corruption, accidental deletion, even sabotage can have a catastrophic effect. The integrated, mission-critical nature of data systems in today's enterprises necessitates significantly more responsive and real time solutions.

In February 2001, Microsoft included Persistent Storage Manager (PSM) in Microsoft's OEM Server Appliance Kit. PSM delivers Live Primary Data Protection for any Server or Appliance running Windows 2000, XP or .NET by creating hundreds of point-in-time disk images (snapshots) of the data volume. The PSM snapshots look like the volume at the time of creation and are kept on the active volume to facilitate the immediate return of individual files, groups of files, folders or complete volumes.

> **"Microsoft's adoption of *Persistent Storage Manager* marks a very strategic transition in the network age, continuous access to data is the key to high availability operations. By embedding PSM, Microsoft has embraced an essential and proven element of data center-class operations and enabled all leading server and storage appliance vendors to provide world-class solutions."**
>
> ***Michael Peterson, President of Strategic Research Corp.***

Columbia Data Products' close relationship with Microsoft has resulted in a PSM that is tightly integrated with the Operating System delivering a level of data protection not available from secondary solutions.

Additional information is available from the Columbia Data Products Website <www.cdp.com/library/PSM/>

2. Could this be the end of Backup as we know it?

PSM's Live Primary Data Protection is integrated directly into the storage environment, running continuously in the background creating new snapshots, deleting older images, maintaining a library of the most recent versions of your work or older archives. PSM is on-line facilitating the immediate return of individual files, groups of files, folders or complete volumes, without the assistance of a Network Administrator (if set up to function that way).

During the first 12 – 24 hours, before the first nightly backup is done, data is at its peak of vulnerability. Analysis of medium and large company infrastructures indicates that less than 20% have the means to protect data during its first 24 hours. During the first 24 hours PSM can create dozens of point-in-time snapshots from which data can be recovered instantaneously!

Nightly backups are usually "incremental", by weeks end you will have five or six incremental backups and one complete backup. Restoring from tape could require all five or six incremental tapes as well as the full backup. During the same period of time PSM could have taken between 50 to 150 snapshots, each complete within themselves, each containing an exact copy of the volume(s) at the time it was taken and it is on-line for immediate access.

A more complete discussion of snapshot scheduling, snapshot utilization and storage requirements is covered later in this paper and in more depth in other CDP Whitepapers. <www.cdp.com/library/PSM/>

3. Snapshots – New Paradigm – New Metrics

In today's world of integrated IT systems, providing real time information and interaction is no longer a luxury but a necessity. Low to mid-range tape drives restore around 85MB/minute and could take over one week to restore a single Terabyte of data. By comparison, PSM is virtually instantaneous.

The current version of PSM supports 250 concurrent snapshots per volume with a total of 63 volumes per snapshot. 250 snapshots afford Network Administrators the flexibility to develop strategies to meet the requirements dictated by their unique situation(s).

Left (Fig. 1) is one example of how a company might deploy PSM:

Company "X" has a significant volume of transactional sales activity in addition to the associated support functions. To eliminate the possibility of having to rebuild the sales activity they take hourly snapshots.

Snapshot retention heuristics are set to retain three full days of hourly snapshots, three weeks of daily snapshots and three months or one quarter of weekly snapshots. The accounting department has requested that an End of Month (EOM) snapshot, just prior to posting be maintained.

This strategy uses 106 of the 250 concurrent snapshots provided by PSM. How much storage will that require? A PSM snapshot is a metaphorical point-in-time disk image. Like a "mirror" it looks

Figure 1 - Example of PSM Snapshot Usage

exactly like the source volume. However, a mirror requires the same storage as the original and the first snapshot requires very little space. Once the first snapshot is taken PSM monitors all drive activity retaining the deleted data required to recreate the last snapshot.

Most OEMs set the default cache file size at 15% of the volume. Because storage usage metrics vary so much from company to company, determining the best storage usage metric requires the user to determine how much new data is written daily and how much data needs to be retained for how long.

4. PSM Editions

PSM/SAK

Primary target for this edition: OEMs interested in developing NAS Appliances. Sold almost exclusively through Microsoft, it is also available through CDP. The SAK edition was designed to integrate seamlessly into the Microsoft's Server Appliance Kit.

PSM/MMC

PSM/MMC was developed for OEM manufacturers of general Windows based servers. PSM/MMC integrates directly into Microsoft's management infrastructure for Windows 2000, Windows 2000 Server, XP and .NET Server. Administrative & management screens for PSM are located under the storage tab in the Microsoft Management Console (MMC) utility.

The core functionality of PSM/SAK and PSM/MMC is identical.

PSM Provider

Plugs into .NET Server's VSS (Volume Shadow Copy Service) infrastructure and provides, in addition to the Microsoft Provider snapshot, PSM's Provider snapshot engine which delivers a higher level of functionality.

5. Operational Overview

Each Persistent Image is a complete point-in-time representation of the data on the volume(s). Like the photograph of a 3000-pound automobile that weighs only ounces, each PTI requires only a fraction of the hard-drive capacity of the original data. PSM does not keep all the data that was ever written. PSM maintains only the data required to maintain a snapshot.

Maintaining the data represented by the snapshots for the purpose of recovering from catastrophic failures is the typical CYA (cover your assets) view of Data Protection. The end-user client providing a simple one-click access to past versions or deleted files is a powerful addition to any network.

PSM, like OTM and other products from CDP, works below the Operating System as a Filter Driver at the Volume block level. PSM maintains a library of Persistent True Images, each representing a specific point-in-time. PTI's can be accessed by users, administrators or any windows application, and look just like the file/folder view they are familiar with. This capability will have advantages for administrators, but we feel end-users will find their client a more powerful and easier option.

At installation, PSM establishes a cache file within which PSM retains overwritten data required to build a snapshot. The amount of data that changes daily and the length of time you wish to maintain snapshot data determine the size of the cache file. As soon as the first snapshot is taken, PSM will start monitoring all writes. Data overwritten by the system is copied to PSM and saved to maintain the snapshot. The process is referred to as copy on write.

PSM creates and manages up to 250 snapshots per volume with the upper limit of 63 Volumes per snapshot and supports clustering and automatic failover.

6. Ongoing operations

PSM operates below the file system as a storage filter class driver intercepting all writes to the NAS volume. Even though PSM presents File and Folder information to users, PSM operates at the device block level with a default 64-KB granularity. In other words, PSM takes each data block on the PSM-protected Volume and divides it into 64-KB "Granules", which is more efficient than dealing with the complete block.

7. Writing to PSM NAS Volume

When a write request occurs, PSM intercepts and pauses the write, reads the data that is to be overwritten, and saves the data in a Diff Directory within the PSM-specific cache file. After the original data is written to the Diff Directory, the new data is written on the active Volume. This process is referred to as "copy-on-write".

❶ PSM Intercepts and pauses writes

❷ Old data copied from active Volume to PSM Cache

❸ New data written to active Volume
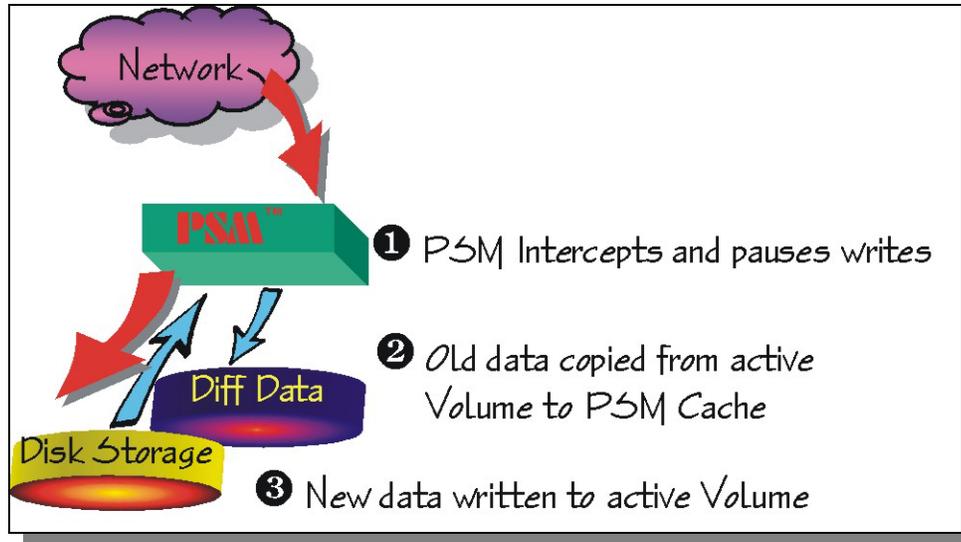
PSM will continue with this "copy-on-write" operation basically copying the overwritten data into Diff Directory.

To conserve cache space, redundant or unneeded changes to a granule are not recorded. PSM keeps only the data required to recreate the snapshots, not all of the activities between snapshots.

8. Reading PTIs

Users who have been granted access by the NAS Administrator see PTIs as network shares.

PTI is a point-in-time representation of the NAS volume at the time it was created. During the copy-on-write operation, the data to be overwritten is preserved in PSM's Diff Directory. When reading a PTI, PSM will determine if the data has changed, meaning it is located in the Diff Directory, or if it is on the live volume. For data that has changed, PSM inserts the original data, held in the Diff Directory and, where no changes have occurred, PSM reads directly from the live volume.

Reading PTIs

❶ Read request from PTI

❷ PSM determines what data is on the active vol & what is in PSM Diff Data

❸ PSM combines the data and presents to user
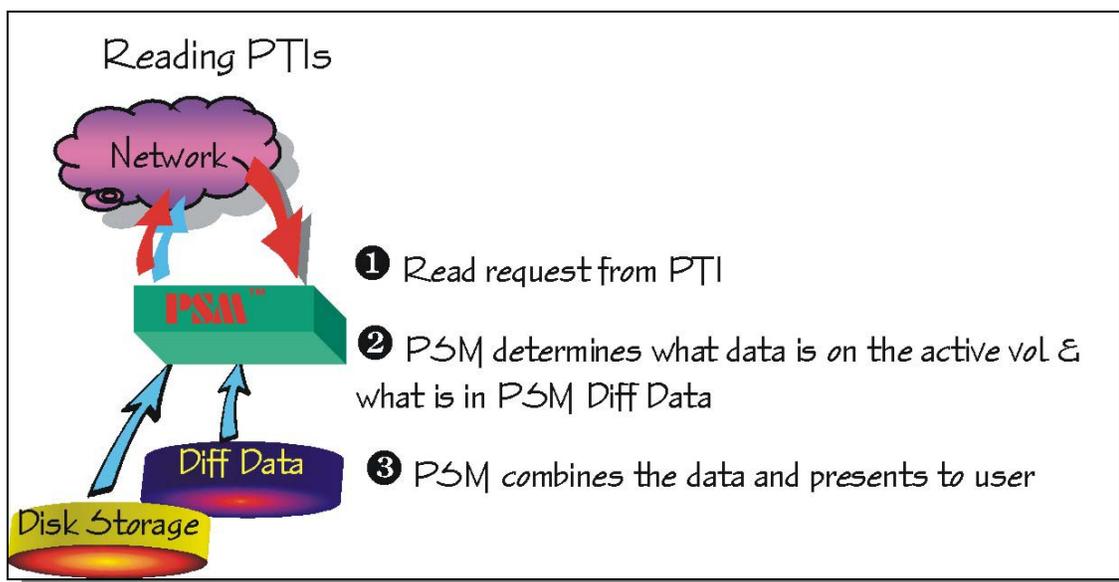
Read requests from the live NAS Volume data pass through unmodified.

Processes, such as backup or restoration having data access through a persistent image, have a lower process priority than the normal read and write operations. Therefore, should a tape backup program be run at the same time the NAS is experiencing heavy client utilization; the tape-backup access to the PSM image is limited while the normal production performance is favored. This helps to minimize normal user impact.

While creating the PSM images happens very quickly, it might take a few minutes before that image is available and visible to the users. In particular, the very first image will generally take much longer to be made available than subsequent images. PSM causes minimal overall performance impact. The NAS Administrator has the ability to change the names of the directories.

9. Creating PTI

Creation of Persistent True Images is scheduled through the SA Kit interface or may be generated by the NAS Administrator as a one-time request.

When the command to create a PTI is issued, PSM begins monitoring the file system looking for a quiescent period. A quiescent period is the amount of time a volume must be dormant before a persistent image is created. The default quiescent duration is five seconds but the NAS administrator may configure this, as can the amount of time PSM should search for this inactivity window.

The quiescent period provides sufficient time for completion of writes and for the various software buffers to flush, the premise being that, by the end of the quiescent period, a Volume will be produced which is in a stable state meaning that the Volume is at rest and in a functional condition ready for users to access. If the Volume is captured in a stable state, then that volume, or files and folder contained in the volume, will be returnable in a stable state or "useable condition" to users.

CDP has been using this process for years in CDP Backup software and in an OEM offering called Open Transaction Manager . OTM is the industry's leading open file agent and is used by a number of software developers, including Veritas in NetBackup and Backup Exec.

Following the quiescent period, PSM creates the Persistent TrueImage. The PTI is a virtual point-in-time representation of the volume. From the user perspective, the PTI provides a directory structure that exactly replicates the NAS at the PTI's creation. Metaphorically, the PTI contains the data that was overwritten on the live volume from the time of the previous PTI creation to the creation of the current PTI.

In reality, at the time of PTI creation, PSM sets up junction points to the Diff Data maintained in the PSM area. The actual creation of the PTI requires minimal resources and very little time.

10. PSM Snapshot Attributes:

READ ONLY, READ/WRITE., ALWAYS KEEP

Additional information on the uses of PSM is contained in documents found at <www.cdp.com/library/PSM/>

READ ONLY

The default setting is for PSM to create "READ ONLY" snapshots which prohibits any modification to the PTI (snapshot) – this is the most common parameter for snapshots. A READ ONLY snapshot allows users, who have been granted access, to view, open and save a copy of any file represent in the snapshot. The properties of a READ ONLY snapshot may be modified by the NAS Administrator to READ / WRITE or ALWAYS KEEP.

READ/WRITE

The READ/WRITE attribute may be assigned at the time of creation or the NAS Administrator may at any time change the attribute of any snapshot. READ/WRITE snapshots provide some unique capabilities to PSM.

READ ONLY snapshots which were changed to READ/WRITE snapshots and then modified when returned to the original READ ONLY condition will cause all changes go away returning the data represented in the snapshot to the way it was originally, effectively acting as an UNDO.

Other applications for READ/WRITE snapshots: CFO's and auditors can run trial balances to accounting systems without affecting the actual systems. Prototyping; a new version of a program can be installed in a READ/WRITE snapshot and its compatibility within the system tested with no adverse affects to the primary system.

ALWAYS KEEP

ALWAYS KEEP snapshots are treated as sacrosanct by PSM. In a cache file fill situation PSM will cease writing to the cache file to avoid deleting or corrupting an ALWAYS KEEP snapshot. A "disk full" error will be returned to the user. ALWAYS KEEP allows the administrator to set some milestones that are not subject to the automatic deletion routines.

11. Automated snapshot deletion

PSM has a snapshot weighting system (low to highest) that helps set the priority of the PTI. This weighting combined with the age of the snapshot determines the order by which PTIs will be deleted by PSM when the cache file fills up.

A key fact to consider is that PSM provides Primary Data Protection automatically. Once set up, PSM will continue to provide Data Protection generating new scheduled snapshots or deleting older snapshots with little or no input required from system administrators.

12. Data Recovery

File/Folder/Volume Recovery

PSM facilitates instant data recovery from the stored on-line images. Individual files, groups of files, folders, groups of folders or complete volumes can be restored. Recovering the data can be accomplished by the NAS Administrator or the NAS Administrator can give individual users access to their data for that purpose.

Security rights and privileges, as well as file and directory attributes, remain in effect as they were at the time the snapshot was created.

13. Virus Infection and Persistent True Images

A computer virus, like a human virus, usually has an incubation period — sometimes destruction starts slowly and other times its action is rapid. But in either case, with PSM's Live Primary Data Protection the System Administrator is able to "roll back the clock" to a pre-infection Persistent Image. In the event the pre-infection milestone is unknown, the System Administrator has the ability to examine each of the Persistent Images before making the decision. Even after selecting a snapshot, the ability to move forward or backward to other snapshots is retained.

14. VSS / Volume ShadowCopy Service

Microsoft's Volume Shadow Copy Service (VSS) is both an infrastructure and a service that will be available in .NET Server and will not be available in Windows 2000 SAK or Windows 2000 Advanced Server. More information on VSS is available on the Microsoft Website. Information is available on how PSM will compliment VSS functioning as a "PRIOVIDER" can be found at <www.cdp.com/library/PSM/

15. PSM Performance Impact

Write Performance Impact:

PSM creates minimal additional I/O overhead which is limited to writes. The copy-on-write process adds one read (the write is paused to read the old data) and one write (the old data is written to the Diff Directory file) to each write system request.

Read Performance Impact:

Minimally, reads are not affected since typically 90% of all I/O activities are reads directly from the disk with no interaction with PSM. This minimal impact adds tremendous advantages

Additional Operational Performance Metrics

Future updates of this document will include specific metrics on Boot Time, Restore Time, etc.

One very important consideration for optimal performance is to be certain that the latest Service Packs have been installed.

16. Foreign Language Support

Localized editions of PSM/SAK are available in English, Japanese, French, German and Spanish.

Additional language support can be provided at a nominal fee.

II. Persistent Storage Manager Specifications

PSM/SAK Version 2.2 – October 2002

Persistent Storage Manager	
Operating System Support	Windows 2000 Advanced Server w/SAK
	.NET (upon release)
Minimum Memory	256MB
Maximum Memory	4GB
Snapshots per Appliance	250
Volumes per Appliance	255
Volumes per Snapshot	63
Maximum Storage per Appliance	10TB
Hardware RAID	Yes
Software RAID	Yes
Storage Interface	Fiber Channel
	SCSI
	IDE
Dual Processor Support	Yes
Virtualization	Basic and Dynamic LDM in W2k
Volume Type	NTFS Volumes Only
Granule size / Cache file size	64K (default) / 1TB cache
	128K granule / 2TB cache
	256K granule / 4TB cache
Cluster support	2 nodes (W2k)
	4 node (.net)
	Microsoft Cluster Server
Custom versions with different specs available to OEMs from Columbia Data Products	

III. PSM/SAK User Guide

1. Introduction

Persistent Storage Manager, from Columbia Data Products, is an optional add-on package in Microsoft's Server Appliance Kit (SAK). The SAK was developed to provide Hardware OEMs the ability to develop powerful Windows Powered Network Attached Storage (NAS) Appliances with minimal effort.

Tightly integrated with the SAK, PSM brings snapshot functionality, providing Instant Data Recovery from Hundreds of online Persistent Images™ to the SAK based NAS Appliances.

For more information on Persistent Storage Manager consult <www.cdp.com/library/PSM > or email support@cdp.com
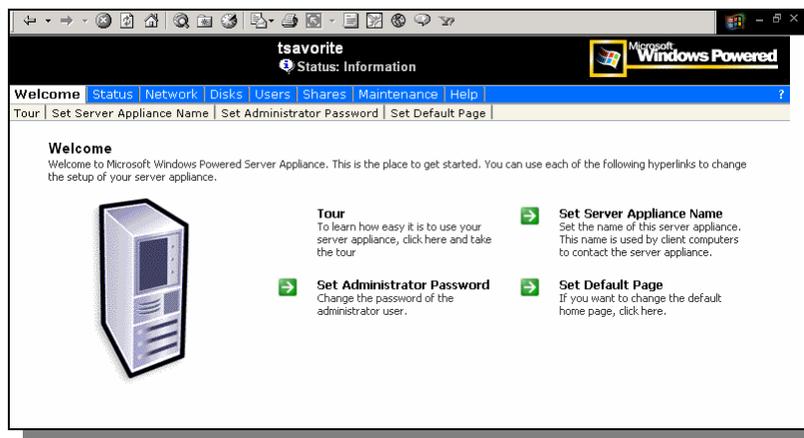
2. Welcome Screen

Figure 1 - Welcome Screen

Figure 1 is the Welcome screen for the SAK, PSM is found under the Disks Tab

Figure 2 - Disks Screen

The storage attached to the SAK is managed from this area, Figure 2, Obtain access to the PSM management area from this screen.

3.   Main PSM Screen
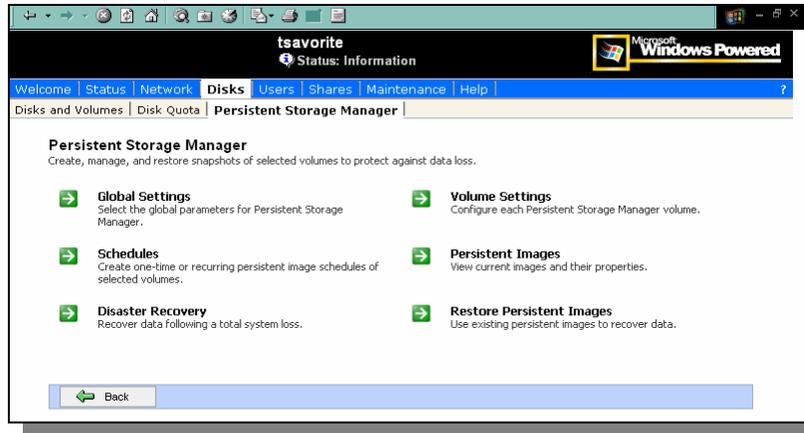
Figure 3 - Main Screen Persistent Storage Manager

Figure 3 – Persistent Storage Manager Main Screen. All of the management and maintenance functions are accessed from this screen

4.   Persistent Storage Manager // Global Settings
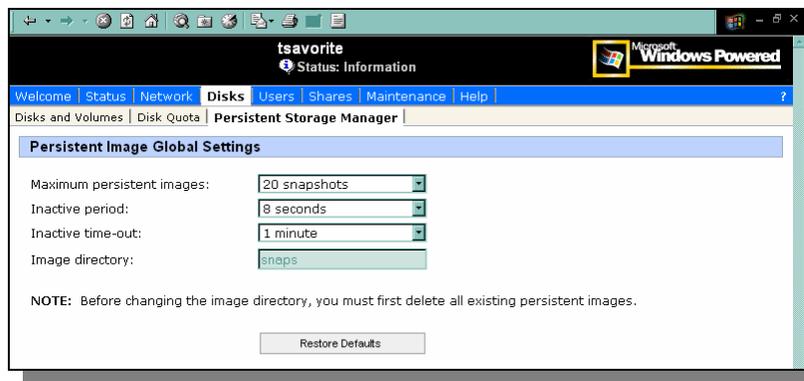
Figure 4 - Global Settings

From the Global Settings screen (Figure 4) you can control the overall environmental settings for Persistent Storage Manager. Some options will be disabled if there are already active persistent images.

Restore Defaults

The Restore Defaults button will reset the system defaults.

Maximum persistent images

Determines the maximum number of active Persistent Images (snapshots). PSM will support a maximum of 250 snapshots per server. The size of the cache file will determine the actual amount each server can hold.

If the creation of a new snapshot would cause the maximum number to be exceeded, the system will delete the oldest existing persistent image according to the deletion heuristics established by the user.

Inactive period

Specifies the amount of time a volume must be dormant before a persistent image is created. Prior to starting a persistent image, the system will wait for the volume being imaged to become inactive. The default value will allow systems to start an image with a consistent file set and a minimal time-out. Administrators can change this value for system optimization. Reducing the inactive period will allow you to create persistent images even on busy systems, but with possible synchronization problems within applications which are concurrently writing to multiple files.

Inactive time-out

Specifies how long the server should try to create a persistent image. A persistent image will not begin until a period of relative inactivity set by the Inactive period has passed. If an interval passes that is longer than the Inactive time-out period, the persistent image will not be created and a notice generated to the system event log.

Image directory

Specifies the root directory used for the persistent image. Each persistent image appears as a subdirectory of the volume that is being imaged. The entire content of the volume as it existed at the moment the persistent image was created will appear under this directory.

5. Persistent Storage Manager // Volume Settings
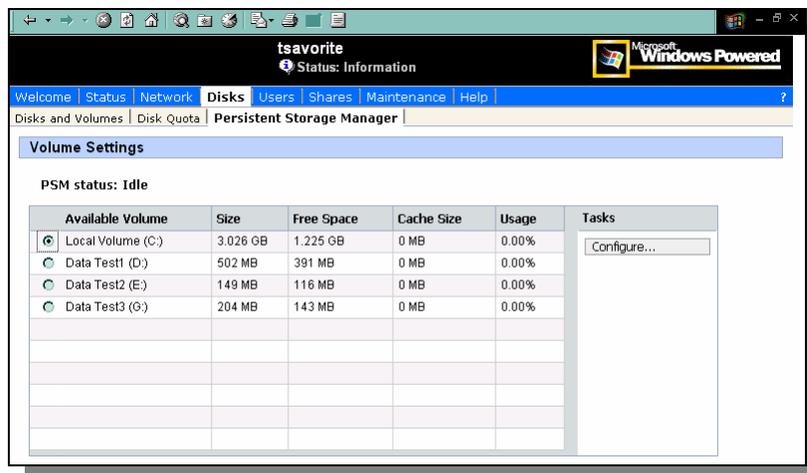

Figure 5 - Volume Settings

From the PSM screen select Volume Settings (Figure 5). From Volume Settings screen you can view the Persistent Storage Manager attributes for each volume and change volume settings using the Configure button in the Tasks list.

Available Volume

Lists all of the volumes that can support persistent images. You can select the volume you want to configure.

Size

Displays the size of the volume.

Free Space

Displays the available storage size of the volume.

Cache Size

Specifies the amount of space allocated to the cache file. Increasing this value will allow more and larger persistent images to be maintained.

Usage

Displays the current cache file use as a percentage of the cache size.

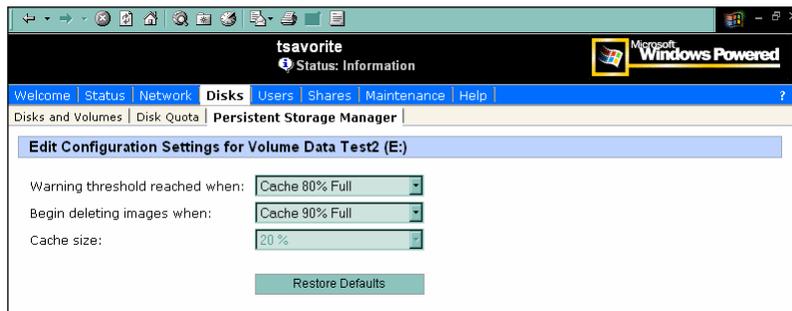# 5a. Persistent Storage Manager // Volume Settings // Configure

Figure 6 - Volume Configuration Settings

Pressing configure from the Volume Configuration screen brings you to the settings screen, Figure 6, where you can modify the various aspects of PSM's volume attributes. Some of the fields will appear read-only if there are active persistent images. The Restore Defaults button will re-establish the system defaults.

Warning threshold reached when

Defines the percentage of cache space which, when consumed, will trigger warning messages to the system event log.

Begin deleting images when

Defines the percentage of cache space which, when consumed, will trigger the automatic deletion of the oldest persistent image on the system. Automatic persistent image deletions are recorded in the system log.

Cache size

Specifies the amount of space allocated to the cache file. Increasing this value will allow more and larger persistent images to be maintained. Make sure that adequate space is available on the drive where persistent images are stored.

6. Persistent Storage Manager // Schedules
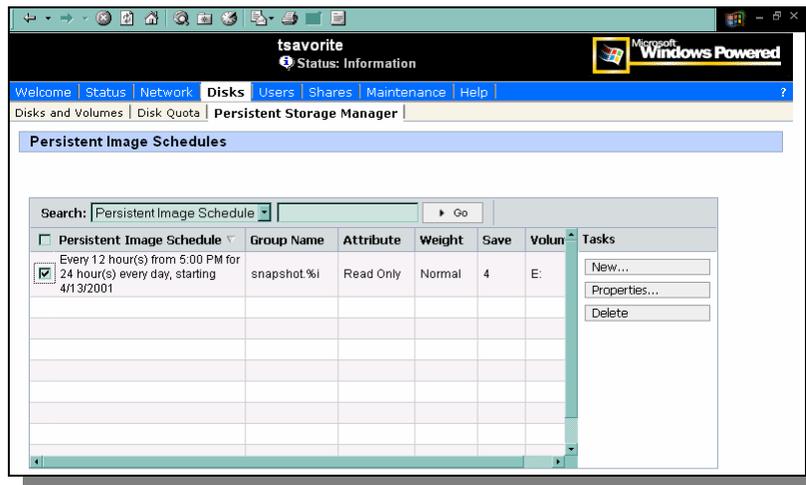
Figure 7 - PSM Schedules

The Persistent Storage Manager Schedules page displays a list of scheduled persistent images and associated tasks.

Each scheduled persistent image contains information such as its scheduled time, day, frequency, starting date, and group name.

Schedules screen allows you to create new schedules, delete existing schedules, and edit schedule properties.

6a. Persistent Storage Manager // Schedules // New
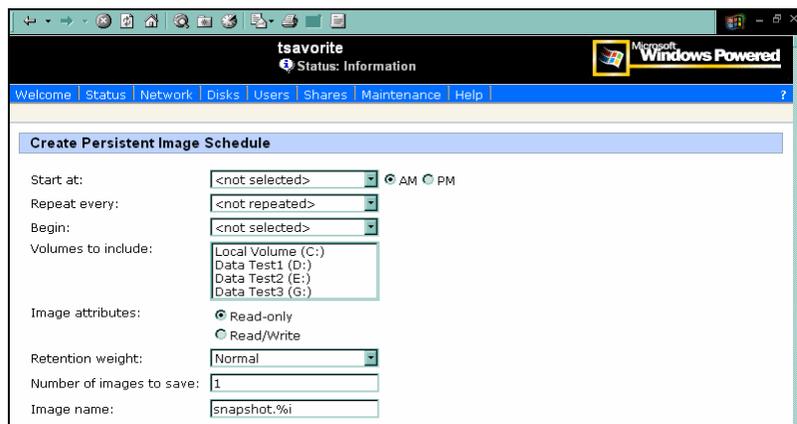
Figure 8 - Create PTI Schedule

Create a New Schedule

To create a new schedule, you must supply a starting time, repeat period, starting day, volume, and the number of persistent images to make available to users.

To add a persistent image to the schedule:

– On the primary navigation bar, choose Disks.

– Choose Persistent Storage Manager.

– Choose Schedules.

– In the Tasks list, choose New.

– Select the parameters you want for the schedule.

– Choose OK.

6b. Editing Persistent Image Schedule Properties
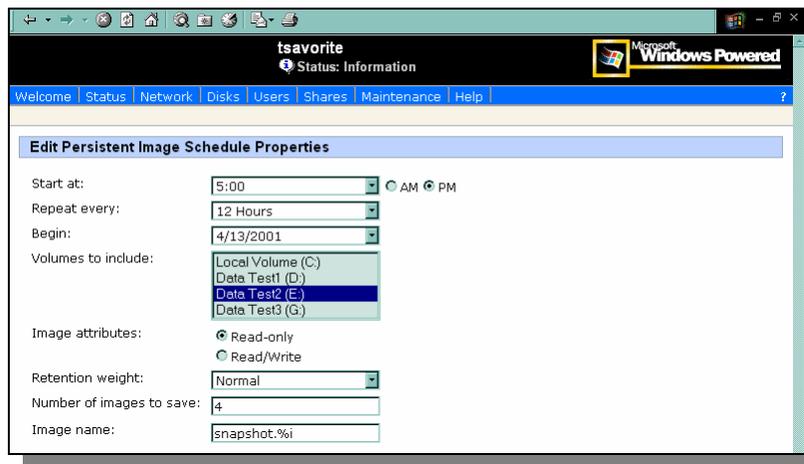
Figure 9 - Edit Schedule Properties

Edit Persistent Image schedule properties:

– On the primary navigation bar, choose Disks.

– Choose Persistent Storage Manager.

– Choose Schedules.

– In the Tasks list, choose Properties.

– Select the changes you want to make to the schedule.

– Choose OK.

6c. Deleting a Persistent Image Schedule
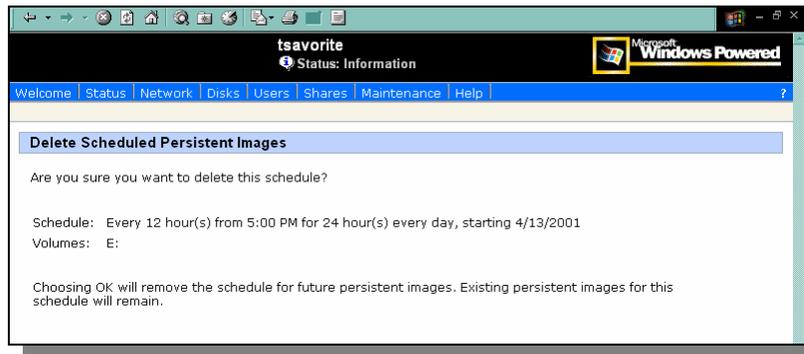
Figure 10 - Delete Scheduled Images

To delete a persistent image schedule:

– On the primary navigation bar, choose Disks.

– Choose Persistent Storage Manager.

– Choose Schedules.

– Select the schedule you want to delete.

– In the Tasks list, choose Delete.

– Choose OK.

7. Persistent Image & Group Information

Figure 11 - Persistent Image and Group information

After a persistent image is created from the schedule you specify, it becomes a member of an image group. The Persistent Image and Group Information page displays the following information about the image group:

Image name and location on volume

Displays the name of the image and its path.

Persistent image group name

Displays the name assigned to this group.

Number of images in group

Displays the maximum number of images that can be included in the group.

Volumes included in this image

Displays each volume included in the image.

Image attributes

Displays the read-only or read/write attribute of the image.

Retention weight

Displays the relative retention weight of the image.

Most recent image in group

Displays the date and time of the image most recently added to the group.

Oldest image in group

Displays the chronologically oldest image in the group.

Next image in group to be deleted

Displays the date and time of the image that will be deleted next so the system can stay within the saved images limit.

7a. Managing Persistent Images

Figure 12 - Persistent True Images

The Persistent Images page displays active persistent images. Each entry identifies the date and time the persistent image was created, the read-only or read/write attribute, the preservation weight, and the volume it preserves.
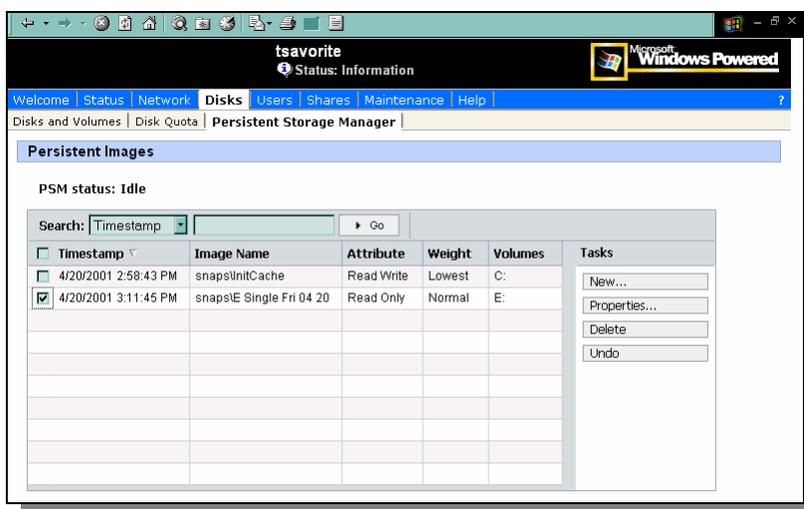
To manage persistent images:

– On the primary navigation bar, choose Disks.

– Choose Persistent Storage Manager.

– Choose Persistent Images.

– Select the persistent image you want.

– Choose one of the following tasks:

– Choose New to create a new persistent image.

– Choose Properties to view or change the image read/write attribute or retention weight.

– Choose Delete to delete the image from the system.

– Choose Undo to undo changes to a read/write image.

7b. Creating a New Persistent Image
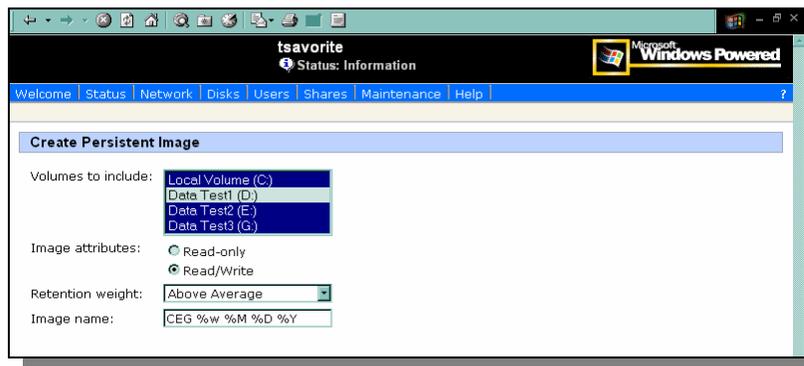
Figure 13 - Create PTI

Persistent images may be created directly through the Persistent Images page. You can also use the Schedules page to schedule future or recurring persistent images. To create a new persistent image:

– On the primary navigation bar, choose Disks.

– Choose Persistent Storage Manager.

– Choose Persistent Images.

– In the Tasks list, choose New.

– In the Volumes to include list, choose volumes to be included in the image.

– Select the Read-only or Read/Write button.

– Select a retention weight from the Retention weight list.

– Type your image's name in the Image name box.

– Choose OK.

7c. Deleting a Persistent Image
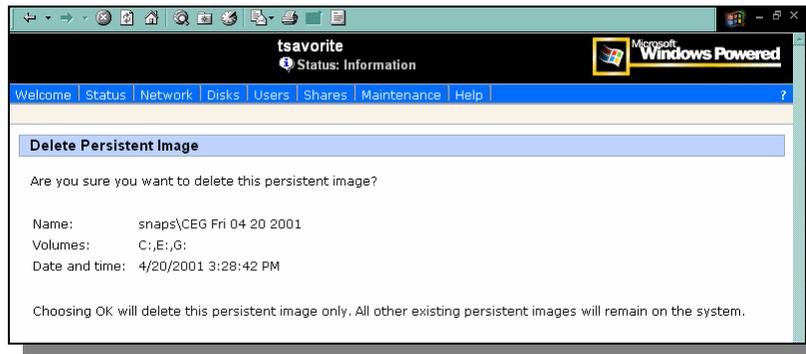
Figure 14 - Delete Verification

To delete a persistent image

– On the primary navigation bar, choose Disks.

– Choose Persistent Storage Manager.

– Choose Persistent Images.

– Select the persistent image you want to delete.

– In the Tasks list, choose Delete.

– Choose OK.

7d. Editing Persistent Image Properties
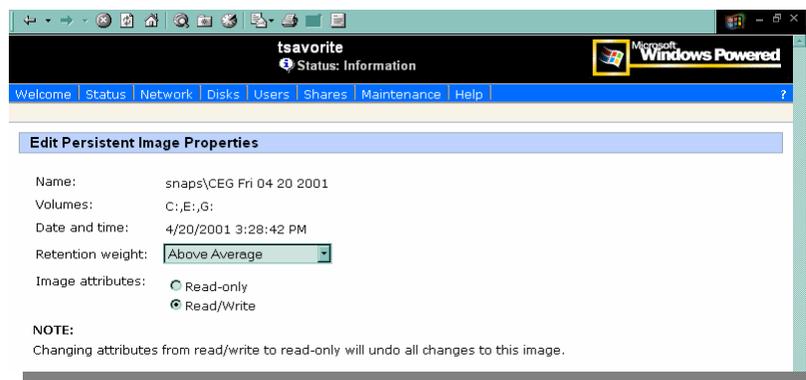
Figure 15 - Edit PTI Properties

You can change properties such as the read-only attribute or preservation weight of an image.

To edit persistent image properties:

Figure 16 - Edit PTI Properties

–   On the primary navigation bar, choose Disks.

–   Choose Persistent Storage Manager.

–   Choose Persistent Images.

–   In the Tasks list, choose Properties.

–   Select a retention weight from the Retention weight list.

–   Select the Read-only or Read/Write button.

–   Choose OK.

7e. Undo Persistent Image Changes
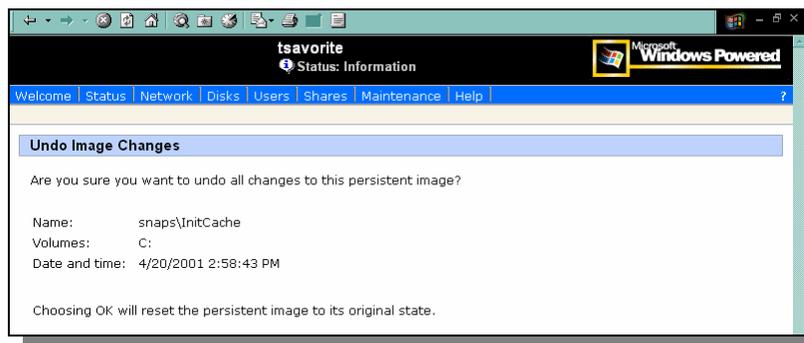
Figure 17 - UNDO Changes to PTI

After you create a read/write persistent image, you can make changes to the image, for example, you can modify files in the image, add new files, or delete existing files. If you make a change to an existing image and later want to revert to the original file contents, you can use the following procedure to restore the original persistent image.

To undo persistent image changes:

–   On the primary navigation bar, choose Disks.

–   Choose Persistent Storage Manager.

- Choose Persistent Images.

- Select the persistent image you want to restore to its original state.

- In the Tasks list, choose Undo.

- Choose OK.

7f. Restoring an Image
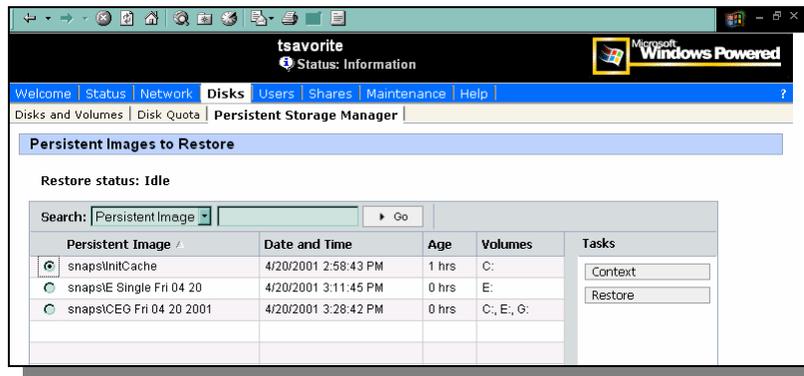
Figure 18 - Images Available to Restore

The Persistent Images to Restore page (Figure 18) displays a list of all persistent images. You can choose to view an image or restore your server appliance to an image you have previously created.

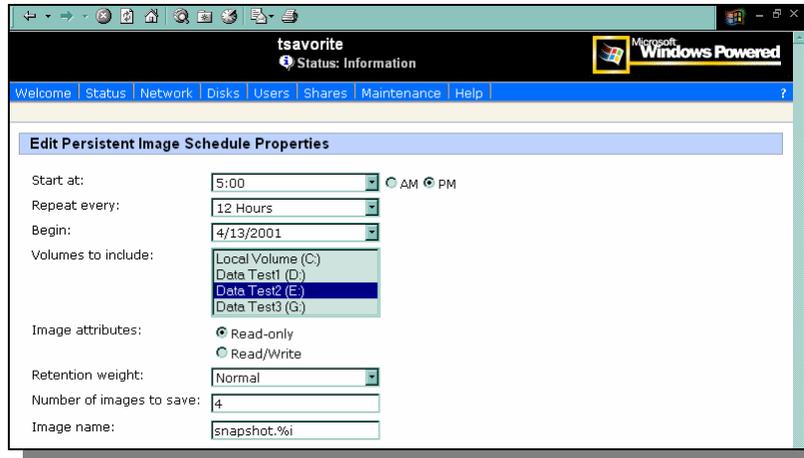To restore a persistent image:

- On the primary navigation bar, choose Disks.

- Choose Persistent Storage Manager.

- Choose Restore Persistent Images.

- Select the persistent image you want to restore.

- Choose Restore.
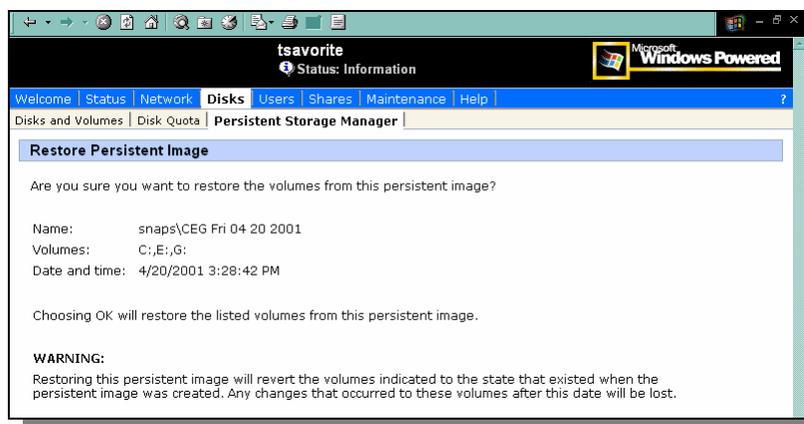
Figure 19 – Restore Confirmation Screen

After selecting Restore the Are you sure (Figure 19) screen will appear.

– Choose OK

8. Persistent Storage Manager // Disaster Recovery (Optional Component)
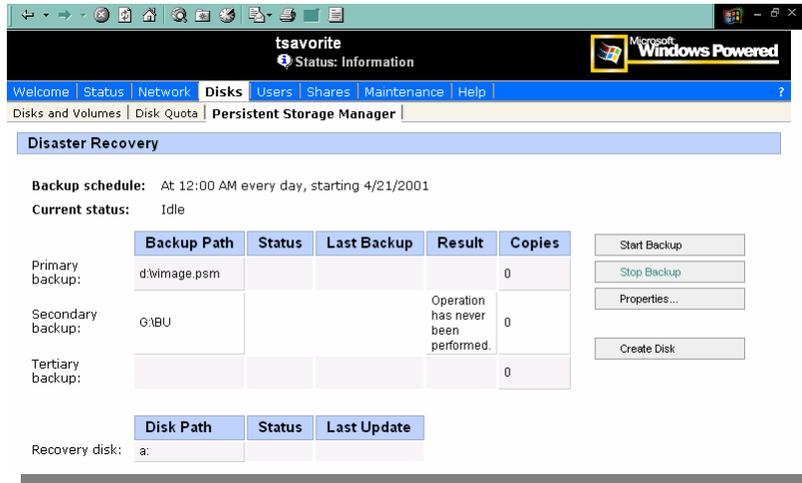
Figure 20 - PSM Disaster Recovery

This page displays the disaster recovery status and provides commands to back up the system volume, modify disaster settings, restore system defaults, and create a disaster recovery disk. After a successful backup to a network share or local hard drive, booting the server using the disaster recovery disk will restore the system volume from the backup image. The restore process does not require any user intervention, and the recovery will be attempted from the first backup path found containing a valid disaster recovery image.

Backup Schedule

Displays date, time and frequency of the disaster recovery backup.

Current Status

Displays the status of the backup engine. If a backup is not in progress this field will display the word 'Idle', otherwise it will display a short message indicating the current backup engine activity.

Backup Path

Displays from one to three network or local drive paths. These are the folders which will contain the disaster recovery backup data. A complete backup will be copied to each of the three destinations. Blank entries are permitted and ignored.

Status

Displays the status of each backup path. If the folder is online and accessible, this field will display Ready; otherwise, it will display a short message indicating the status of the failed connection.

Last Backup

If any backups have been sent to the backup path, this field will display the date and time of the last backup.

Result

Displays the result of the last backup attempt.

Copies

Displays the number of backup images stored on the share or drive.

Disk Path

Specifies the system path to the disk used for disaster recovery. This disk can be local to the server appliance or accessible as a network share.

Status

Displays the status of the disk path. If the folder is online and accessible, this field will display Ready; otherwise, it will display a short message indicating the status of the failed connection. Make sure that a write-enabled disk is in the drive.

Last Update

Displays the date and time of the last disaster recovery disk created.

9. Disaster Recovery Properties (Optional Component)

Figure 21 - Disaster Recovery Properties

This page displays the disaster recovery settings and allows you to make changes.

User Name

The network user name that attaches to the backup shares during a system backup or disaster recovery.

Password

The password for the user.

Path

Contains one to three network or local drive paths. These are the folders which will contain the disaster recovery backup data. Complete system backups can be copied to each of the three destinations. Blank entries are permitted and ignored.

Save

The number of backup copies the system should save. The value should be two or more. If set to one, each backup will erase the previous backup, causing a point in time where no valid backup is available.

Maximum Media Size

The largest single file size that should be created by the backup. This field allows the backup image to be broken into manageable sections for future transfer to CD-ROM, tape, or other external storage.

Backup Schedule

The day, time, start, and frequency for automatic backups. If you select No backups, backups will not run automatically, but can be activated from the DR page.

Backup Name

The name of the backup folder. If you enable multiple backups, a numeric suffix is added to the folder name for each additional backup.

Recovery Disk Path

The path to the disk that initiates disaster recovery. This disk may be local to the server appliance or accessible as a network share.

10. Creating the Disaster Recovery Disk (Optional Component)

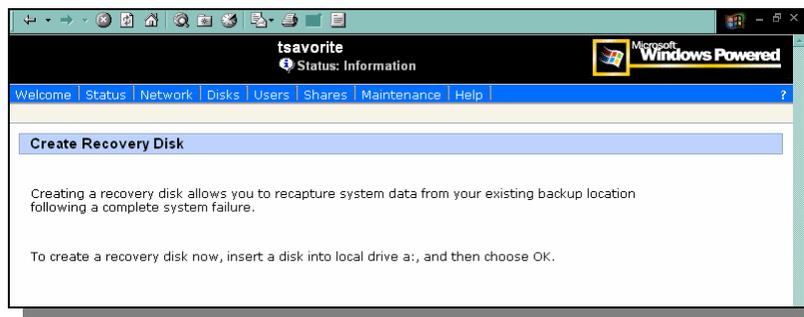

Figure 22 - Create Recovery Disk

The disaster recovery system will create a disk or folder image containing all the files necessary to boot and recover the system volume. Prior to use the files must be copied to a formatted floppy disk and the disk must be made bootable.

To format a floppy disk:

Insert a floppy disk in the diskette drive:

– Run Windows Explorer.

– Choose My Computer.

–   Right Click Floppy (A :).

–   Select Format....

–   Click Start.

–   The system will prepare the diskette to hold files.

To copy files to the floppy disk

–   If you made the disk using the Create Disk button, skip this step.

–   Run Windows Explorer.

–   Select the folder containing the image files.

–   Click the file window.

–   Hold down the CTRL key and press the 'A' key to select all the image files and folders.

–   Hold down the CTRL key and press the 'C' key to mark the files for copy.

–   Choose My Computer in the folder window.

–   Insert a formatted floppy disk in the diskette drive.

–   Click Floppy (A :).

–   Click the file window.

–   Hold down the CTRL key and press the 'V' key to write the files to the floppy.

To make the floppy disk bootable

–   Insert the formatted floppy disk in the diskette drive.

–   Run Windows Explorer.

–   Choose My Computer.

–   Click Floppy (A:).

–   Double-Click the icon labeled FixBoot.

–   A console window will open. Press any key to make the disk bootable.

–   After the console window closes, remove the floppy disk.

II. Cluster / Failover

Cluster Support

PSM supports a 2 node cluster environment.

PSM supports a fail-over of an original volume along with all snapshots to another node in an MSCS cluster. After failure of a node that owned a volume, the surviving node is able to automatically mount the volume, and mount all existing snapshots on the volume.

This implementation is hardware independent and does not require a different code base. There is a single version of the product that can detect the presence of Cluster Service and in case it detects a cluster installation, activates appropriate components.

12. Installing Persistent Storage Manager v2.2

PSM can be installed using one of the following two methods:

Server Appliance Software Update

Server Appliance Software Update (FULL INSTALL via CAB file)

Server Appliance Software Update

This installation method is designed for end users. It allows the administrator of a NAS appliance to install PSM on an appliance already deployed.

The Server Appliance Kit Software Update allows an Administrator to install specific software components to the Server Appliance Kit. The administrator should first place the cab file psm_XX2261.cab for the PSM product setup and XX_psmlang_2261.cab for the PSM Language setup on the workstation.

- Step 1. Copy setup file and/or language setup file to a local folder.
- Step 2. Login to the Server Appliance using a Web browser.
- Step 3. Select Maintenance tab.
- Step 4. Select Software Update option.
- Step 5. Using the Wizard, browse for the location of the PSM CAB file on the workstation or enter full path of the CAB file
- Step 6. Validate the software update package by clicking on the Validate button
- Step 7. Install and Finish the PSM Installation process.
- Step 8. Repeat the process for PSM Language setup.
- Step 9. Repeat the process to install any necessary QFEs.
- Step 10. Restart the system (reboot).

MS Installer Package (FULL INSTALL via MSI file)

This installation method is designed for an OEM engineer building a master image of an appliance.

PSM can be installed directly during the creation of the appliance image by applying two MSI packages:

1. psm_XX2261.msi

This package installs the Persistent Storage Manager package and English language resources.

2. XX_psmlang_2261.msi

This package can be used to install additional language resources for Japanese, German, French and Spanish.

- Step 1. Login to the Server Appliance.
- Step 2. Copy both MSI package files to a local folder.
- Step 3. Double click on psm_XX2261.msi file. This will install the PSM product and English language resources. To install it in unattended mode run this command:

     msiexec /i "psm_ms2261.msi" SAKSU="Yes" REBOOT="Suppress" PSMUNDO="No" ALLUSERS=1 /qn

- Step 4. Double click on XX_psmlang2261.msi file. This will install the additional language resources.

msiexec /i "langsetup_ms2261.msi" ADDLOCAL="All" ALLUSERS=1 /qn

– Step 5. Install any necessary QFEs.

– Step 6. Restart the system

13. Upgrading Persistent Storage Manager 2.2

CAB UPGRADE – QFE Q328158

* PSM Release 1.0 cannot be upgraded to 2.2 directly. The PSM 1.0 product must be removed before installing PSM Release 2.2

* PSM Release 2.0 must be upgraded to PSM 2.1 prior to upgrading to this PSM Service Pack 1

* PSM Release 2.1 can be upgraded to Persistent Storage Manager 2.2 by applying the PSM Service Pack 1.

   All existing Persistent True Images and schedules will be preserved.

Steps to update from PSM Release 2.1:

– Step 1. Copy setup PSM Service Pack 1 CAB file to a local folder.

– Step 2. Login to the Server Appliance using a Web browser..

– Step 3. Select Maintenance tab.

– Step 4. Select Software Update option.

– Step 5. Using the Wizard, browse for the location of the PSM CAB file on the workstation or enter full path of the CAB file Q328158.cab.

– Step 6. Validate the software update package by clicking on the Validate button

– Step 7. Install and Finish the PSM Installation process.

– Step 8. Restart the system.

– Step 9. Repeat the process to install QFE Q328381.cab

14. Uninstall Special Instructions

Step 1: Log on to the PSM server as Administrator

– Login to the Server Appliance Kit browser screen

– Select Disks tab

– Select Persistent Storage Manager tab

– Select Schedules task

– Delete all schedules

Step 2: Remove all network shares associated with PSM images

– Right click on My Computer

– Select Manage

– Open System Tools

– Open Shared Folders

  - Open Shares

  - Remove all network shares associated with PSM Images

Step 3: Delete all PSM images by performing these steps

  - Login to the Server Appliance using a Web browser

  - Select Disks tab

  - Select Persistent Storage Manager tab

  - Select Persistent Image task

  - Select and delete all images

Step 4: Uninstall PSM Application by performing these steps

  - If PSM was installed via an MSI script method or via the SAK Software Update CAB file, perform the following steps:

  - Click the Start button

  - Click on Settings Menu

  - Click on Control Panel

  - Click on Add/Remove Programs

  - Select "Persistent Storage Manager"

  - Click Remove

Step 5: Delete all PSM cache files and cache directories.

  - The following steps must be performed for each existing volumes. Assuming "x" is the drive letter of each volume, perform:

  - Open up a Shell Command Prompt on the PSM server

  - cacls "x:\Persistent Storage Manager State" /g Everyone:f

  - attrib "x:\Persistent Storage Manager State" -r -h -s

  - cacls "x:\Persistent Storage Manager State*.psm" /g Everyone:f

  - attrib "x:\Persistent Storage Manager State*.psm" -r -h -s

  - del "x:\Persistent Storage Manager State*.psm"

  - rmdir "x:\Persistent Storage Manager State"

Step 6: Reboot

PSM Files

Driver

Service

CLI

Data Files

Cache Files

IV. PSM / FAQ

Frequently Asked Questions about PSM are available at the URL below.

www.cdp.com/library/PSM/tech/PSM FAQ.pdf

V. Performance

1. General Comment on Performance and Usability

Two factors will increase the general performance and the usability of any NAS Appliance running PSM. Memory and Cache file size.

Memory

As the capacity of storage devices increases, PSM's Live Primary Data Protection becomes increasingly more important. Handling the larger capacity storage arrays taxes system resources. Additional memory capacity dedicated to PSM can be added to the Appliances – if you are planning some extremely high capacity drives talk with Microsoft or CDP Engineering about your options.

Cache File Size

Storage is cheap – most of us in the storage industry are all too familiar with that song. Dedicating a larger percentage of the machine's hard-drive as PSM Cache File will permit users to keep more snapshots greatly enhancing the user experience.

2. Cache File Size Recommendation

There is some overhead data required for each new Persistent True Image™ within the Persistent Storage Manager™ cache file. This amount is dependent on the size of the PSM granule size of the system. If this amount were not accounted for when creating the cache file, it would fill up the cache file causing automatic deletion of PTIs. It is recommended that this overhead amount be taken into account when the cache file is created.

RECOMMENDATION

Depending on the PSM Granule size used, the following is suggested as the recommended Cache file size:

PSM Granule Size	Recommended Cache File Size[1]
64KB	20% of volume size + 250 MB
128KB	20% of volume size + 500 MB
256KB	20% of volume size + 800 MB

[1] 20% is a recommended percentage for a typical system. For an environment that experiences heavy write I/Os, this percentage may need to be increased.

VI.   Maintenance & Trouble Shooting

1.   General Maintenance

There is no required regularly scheduled maintenance.

Support Contacts

OEMs who obtain Persistent Storage Manager directly from Microsoft have Microsoft as the first level of support.

QFE (Quick Fix Engineering)

The easiest way to limit technical support problems is to be certain to keep up with the latest QFEs, Service Packs, and Releases and implement them as quickly as possible.

How to Obtain Service Packs, etc?

OEMs obtaining PSM from Microsoft will get the QFEs from Microsoft. QFEs released and distributed by Microsoft have been tested and qualified by Microsoft.

2.   Support Procedures

Persistent Storage Manager – Event log messages

If you experience problems in using the Persistent Storage Manager, the following list of event log messages can be used to troubleshoot those problems. Each of these messages is logged to the system event log by the file system driver for Persistent Storage Manager, PSMAN5 driver; each entry appears with "psman5" as the source name.

Complete list of Event Log Error Codes lovated at: www.cdp.com/library/PSM/tech/errorcodes.pdf

If you are unable to correct the problem with the information obtained from the Error Codes contact Technical Support:

End User Support: Contact Vendor
Microsoft OEMs   Contact Technical Support at Microsoft
CDP OEM Support   support@cdp.com

Required information for OEM support

PSM Version and environment (OS version, SAK version, etc…)
CPU Configuration (Processor, RAM, etc)
Storage Configuration (Capacity, Raid (Hardware/Software 0, 1, 5), SCSI, Fiber Channel, IDE, etc)
Any other driver level applications installed
Problem description
Steps to reproduce
System Event Log
If a BSOD issue, we will need a core dump

VII.   Known Issues

Re-extended Volume Revert Error

If a re-extended volume containing True Images of the pre-extended volume is reverted, the re-extended area of the disk will be unusable. To reclaim this space, make sure the included utility "reextend.exe" is executed after reverting from a True Image of the pre-extended volume. Usage of this utility is available by typing "reextend -?".

This utility is available in the directory "c:\winnt\system32\serverappliance"

Failover not available during revert

Cluster service's normal behavior for a volume that can no longer be accessible is to fail-over to another node. During an image revert operation, PSM must disable the target volume. By disabling the volume, Cluster service assumes that the volume has failed and proceeds with a fail-over while PSM is reverting the image. Therefore, you may want to increase the Cluster's default Pending Timeout value to a number comfortable to your specific system.

Cluster revert timeout error

During a PSM revert operation under the Cluster environment, if the volume times out and is made unavailable, the revert operation could not finish and data on the original volume will be incomplete. In some cases, the volume could no longer boot. However, at this point, re-issuing the PSM revert operation and allowing it to finish will get the volume back to its previous state. The following shows the possible eventlog messages that you may see relating to this issue: "Persistent Storage Manager recovery encountered error 3221226026 inserting key (20A0C7:FB) into dictionary. "

"D:\snapshot\snapshot.0 is not accessible. The disk structure is corrupted and unreadable."

Event log error at cache full

The eventlog error "a driver below this one has failed in some way for" may occur when the cached file is full.

Display Error on SAK

Status events not rendered properly on SAK. The percent signs not displayed value substitutions missing in displayed message

Always Keep error at cache file full

If all your Persistent True Images on "C:\" tagged as Always Keep, and the cache file fills up, the system may experience a BSOD at reboot.

It is not recommended to flag all Persistent True Images as Always Keep because this disallows PSM's deletion logic to delete the older Persistent True Images to free up cache file space.

Improper display of default Cache File Size

Default cache setting not being displayed correctly - Volume setup page, pick cache file %, say 2% then take a Persistent True Image. The value grays out and is not selectable. If you hit restore default settings, it will change to 20%. Then hit OK and go back to that page and the screen will say 2% not 20%.

You must delete all Persistent True Images before changing the Cache size.

Page file setting

The Page file size must not change and the initial size must be set equal to the maximum size. This setting is located in the Virtual Memory settings under System Properties.

No Boot – No Revert

If the system cannot boot, a revert operation cannot be performed.

Reverting of System Drive Prohibited

PSM automatically disables the ability to revert the system boot drive. Please call CDP for information on Disaster Recovery option that specifically addresses this issue.

No support for mount points in UNIX

 Microsoft confirmed that the Microsoft's NFS Services for UNIX does not support volume mount points. The NFS clients will not be able to access data on volumes mounted using a volume mount point. Since Persistent True Images for a volume are mounted as directory junctions (AKA mount points), and even though they are shared using NFS, the NFS clients will not be able to access the Persistent True Image data.

Please refer to Microsoft's Release Notes for Microsoft Server Appliance Kit dated June 20001.