VERITAS Storage Migrator Remote™ 3.4.1

System Administrator's Guide

Windows NT

January 2001
30-000072-011

VERITAS

Disclaimer

The information contained in this publication is subject to change without notice. VERITAS Software Corporation makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. VERITAS Software Corporation shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

Copyright

Printed in the USA, January 2001.

VERITAS Software Corporation.
1600 Plymouth St.
Mountain View, CA 94043
Phone 650.335.8000
Fax 650.335.8050
http: / / www.veritas.com

Contents

Figures

Tables

Preface

Introduction

This guide provides a basic functional description of VERITAS Storage Migrator Remote for Windows NT, along with procedures for configuring, managing, and using this product.

The term *VSM* is used for VERITAS Storage Migrator Remote for Windows NT in this guide.

The purpose of this guide is to provide the system administrator with supporting information to help with configuring, using, and managing this product.

Audience

This guide is intended for system administrators responsible for configuring and maintaining systems using Windows NT.

This guide assumes:

- A basic understanding of system administration
- A basic understanding of hierarchical storage management

Organization

This guide is organized as follows:

- Chapter 1, “About Storage Migrator Remote,” defines hierarchical storage management, and describes the key functions of Storage Migrator.
- Chapter 2, “Configuring Storage Migrator Remote,” describes how to do the initial configuration of Storage Migrator after you have installed it. Configuration is done through Storage Migrator’s administrator interface.
- Chapter 3, “Managing Storage Migrator Remote,” describes how to modify the configuration at any time to administer or manage your file space more effectively. Reconfiguration is done through the Storage Migrator’s administrator interface.

- Chapter 4, “Using Storage Migrator Remote,” explains those operations that users may perform with Storage Migrator. These operations are done through Windows NT Explorer.
- This guide also includes the following appendices, a glossary, and an alphabetical index.
  - “Moving VSM to a New Computer” on page 64
  - “Filter Units of Measurement” on page 69
  - “Running Storage Migrator Remote on MSCS Cluster Failover” on page 71

Related Documents

The following documents provide related information:

- *VERITAS Storage Migrator Remote Release Notes* contains a list of supported platforms and storage devices, known problems, and other information not documented elsewhere.
- *VERITAS Storage Migrator Remote Getting Started* describes how to install Storage Migrator.
- *NetBackup BusinesServer System Administrator’s Guide - Windows NT/2000*

  Explains how to configure and manage NetBackup BusinesServer on a Windows NT / 2000 system.
- *NetBackup DataCenter System Administrator’s Guide - Windows NT/2000*

  Explains how to configure and manage NetBackup DataCenter on a Windows NT / 2000 system.

Getting Help

- For license information or information about VERITAS service packages, contact VERITAS Customer Support.

  US Customers: 1-800-342-0652

  International Customers: +1 (650) 335-8555

  Fax: (650) 335-8428
- VERITAS Customer Support can also be reached through electronic mail at:

  `support@veritas.com`

About Storage Migrator Remote 1

Hierarchical Storage Management

Hierarchical storage management is a technique that manages file space more efficiently and expands it beyond conventional system limitations. It increases the availability of critically important data by ensuring that only frequently used information is kept permanently online. Infrequently needed data in the managed file system is migrated automatically to other storage resources, including large-scale data repositories on remote servers. References to the migrated data remain visible online.

When migrated data is accessed by users or applications, it is recalled rapidly to primary online storage. By managing the file system in this way, hierarchical storage management improves system backup performance and releases disk space for application usage. With VERITAS products, data migration is transparent and recall is fast.

Using hierarchical storage management, a managed file system can grow virtually without limit, no longer bounded by the capacity of the online disk(s) upon which it resides.

Although not a substitute for backing up file systems, hierarchical storage management solutions from VERITAS can reduce network traffic and simplify backup administration by shrinking the backup window.

About Storage Migrator

Storage Migrator is a hierarchical storage management product that increases the amount of file space available to users by migrating files from a local Windows NT file system to a secondary store as space is needed in the local file system. When a user accesses a migrated file, it is automatically retrieved from secondary storage and staged in the online file system. Except for the delay to perform the retrieval, users and programs are unaware that file migration and staging are taking place.

This release of Storage Migrator Remote for Windows NT supports two types of secondary stores.

- Folder stores

  Folders can be local to the Storage Migrator Server or they can be folders on remote Windows NT systems that are shared to the Storage Migrator Server.

- FTP stores

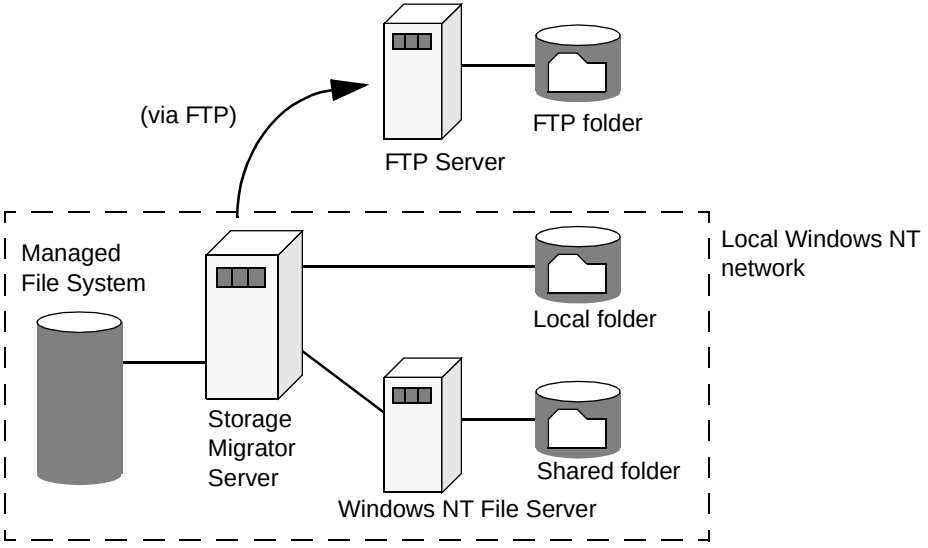
  Storage Migrator supports FTP servers from many different vendors. Files on FTP servers are migrated and retrieved by using standard FTP commands to access the remote file system.

Future releases of this product will support other types of secondary stores, including a variety of removable media stores. For more information, see “Stores” on page 6.

In the example of a basic Storage Migrator configuration shown in Figure 1, a managed file system resides on the Storage Migrator Server. The Server migrates files to secondary store folders on the local system or on an FTP server. A copy of VERITAS Storage Migrator for UNIX or VERITAS Storage Migrator for Windows NT can be running on the FTP server. It is also possible to migrate files to a folder on a different Windows NT server in the local network by sharing that folder to the Storage Migrator Server.

Note Storage Migrator can only manage local NTFS file systems, not file systems shared from other Windows NT servers.

Figure 1. Basic Storage Migrator Configuration



There are two main steps in the migration process. In the first step, Storage Migrator selects files according to predefined selection criteria and copies the file data to one or more secondary stores. In the second step, Storage Migrator automatically purges the copied file data, thereby freeing space in the managed file system. Until files are purged they remain available on disk. Files are not considered to be fully migrated until they have been purged. See “File Migration” on page 4.

Purging occurs whenever the file system is filled to a point where the remaining free space is less than the targeted free space or the file system becomes full. After purging, the filename and attributes of each migrated file still remain in the user’s directory. Information about each copy of each migrated file resides in a database maintained by Storage Migrator. See “File Migration” on page 4.

If a user accesses a migrated file, Storage Migrator makes it available by staging the data back to disk. See “File Staging” on page 6.

The remaining topics in this chapter provide an overview of the tasks that Storage Migrator administrators and users can perform. There is also a functional overview that provides a more detailed explanation of how Storage Migrator operates.

Administrative Controls

The Storage Migrator administrator configures and manages the operation of Storage Migrator through the administrator graphical user interface (Administration interface). The administrator can choose the file systems that Storage Migrator manages and tailor Storage Migrator to meet the migration requirements of those file systems.

Areas that the administrator can configure for each file system include:

- File space threshold (percent free space) targeted by Storage Migrator.
- Criteria that Storage Migrator uses when selecting individual files to migrate.
- Which secondary stores will hold copies of migrated data.

See “Configuring Storage Migrator Remote” on page 11 and “Managing Storage Migrator Remote” on page 41 for more information.

User Controls

The administrator can grant users some control over the migration and staging of their own files by allowing them to:

- Force the migration of specific files.
- Stage specific files.

See Chapter 4 for additional information.

Functional Description

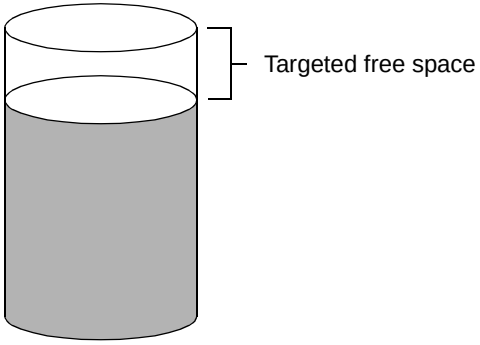
The introduction to this chapter provides an overview of Storage Migrator. The following topics provide a more detailed description of how Storage Migrator operates:

- Disk-Space Management
- Basic Operations and Features
- Stores
- Migration Policies
- System Operations

Disk-Space Management

With Storage Migrator, you can set certain migration parameters and the system automatically makes file space available when the need arises. Storage Migrator attempts to maintain a configurable amount of un-utilized file space on disk. This is called *targeted free space*. Migration operations begin whenever the actual free space becomes less than the targeted free space.

Figure 2. File System Space Threshold



Basic Operations and Features

- File Migration
- File Staging

File Migration

During file migration, Storage Migrator first selects files and copies the file data to secondary storage, and later purges file data as needed. Purging may occur as soon as all copies of a file have been made.

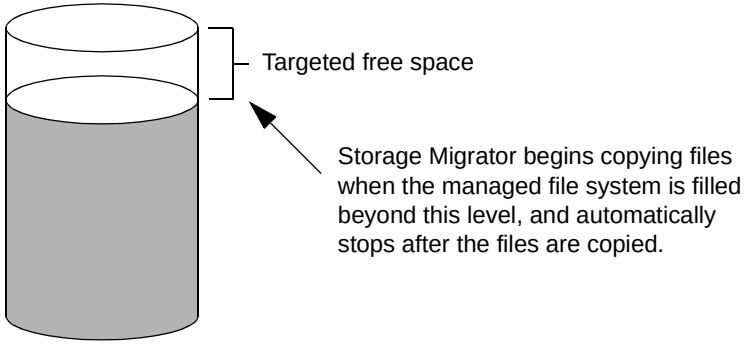
Select and Copy Files

Storage Migrator selects files by sweeping the managed file system and evaluating each file against the migration criteria configured for that file system. These criteria typically include attributes such as file size and file age. Files that meet all of the criteria become candidates for migration. See “Filters” on page 8.

Storage Migrator maintains an inventory of migration candidates, and first copies the best candidates to secondary storage as determined by a configurable migration parameter that weighs file size and file age. See “Folders to exclude from migration” on page 16.

Copying starts whenever the actual free space is less than the targeted free space and no previously migrated files on disk remain to be purged. Copying continues beyond the amount necessary to obtain the targeted free space. This leaves an inventory of migrated data on disk that is available for purging the next time actual falls below the targeted free space.

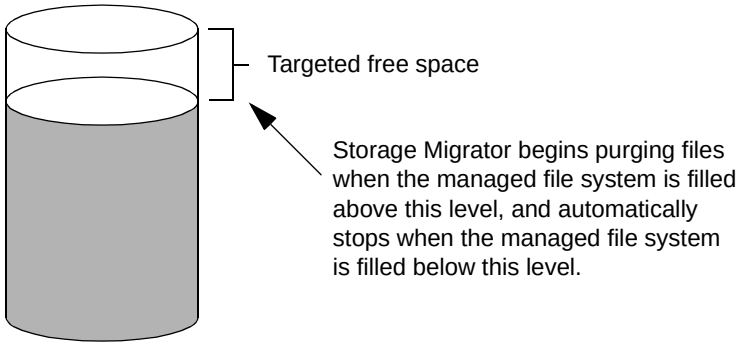
Figure 3. File Migration, Copy Operation



Purge Files

During file purging, Storage Migrator selects migrated files that are copied and removes this file data from disk, making additional file space quickly available. This occurs whenever the actual free space is less than the targeted free space. Purging stops whenever the actual free space is greater than the targeted free space.

Figure 4. File Migration, Purge Operation



The names of all migrated files remain in their original directory and stay visible to the user.

File Staging

Staging (sometimes called *caching*) is the process of copying migrated file data back to the managed file system for access.

Because files are not fully migrated until they have been purged, files that have been copied to secondary storage but not yet purged remain fully accessible and there is no staging delay. Otherwise, the staging process copies the migrated data back once from secondary storage to the managed file system and recreates the file in its original directory.

Storage Migrator blocks file access on all `read` and `write` requests until the migrated files are fully staged.

Stores

Stores are defined in Storage Migrator as a set of like media used to hold copies of file data. Anything capable of holding or providing data appears to Storage Migrator as a store, regardless of its physical characteristics.

There are two types of stores: primary and secondary. Primary stores are those to which the user has access, such as file systems. Secondary stores are used by Storage Migrator to store copies of data, and are not directly accessible by users. Depending on their type, some stores can be either primary or secondary.

Both primary and secondary stores can be managed by Storage Migrator. A store becomes managed when policies are applied to it. See “Migration Policies” on page 7.

The following store types are supported in this release:

- File System Stores

  File systems are primary stores. NTFS file systems can be managed in this release. FAT file systems must be converted to NTFS before they can be managed.

- Folder Stores

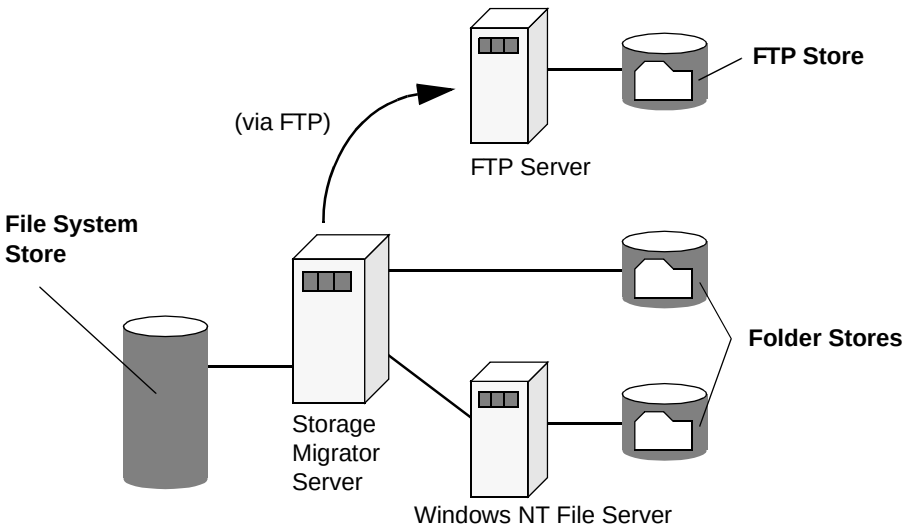
  Any folder accessible from the Storage Migrator Server can be used as a store.

  Data in a folder store will be compressed if the underlying file system (NTFS) supports it.

- FTP Stores

  Any folder on a remote server accessible through standard file transfer protocol (FTP) can be used as a store.

Figure 5. Store Types



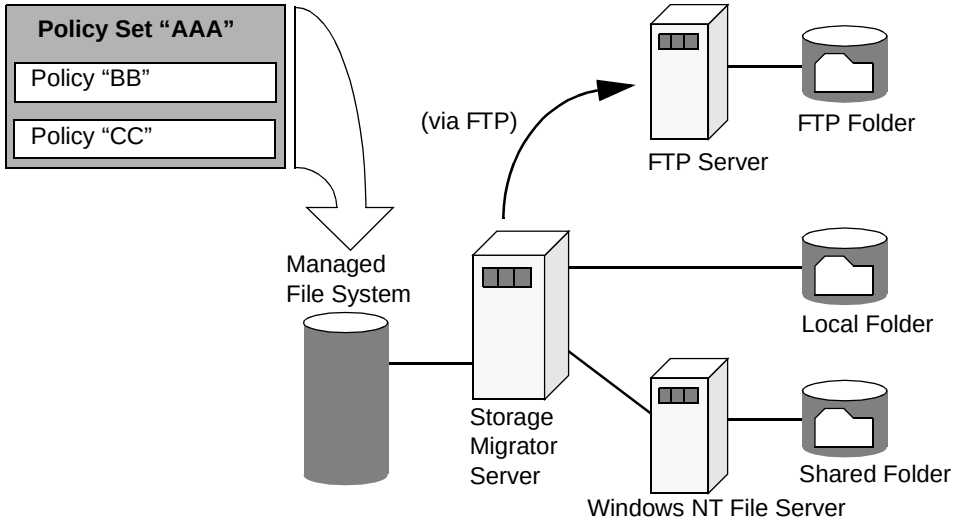
Migration Policies

Configurable migration policies specify *which* files can be migrated and *where* they will be migrated. Policies define the exact operations Storage Migrator performs on a managed store. One or more policies comprise the policy set that applies to the managed store.

Different types of policies specify different types of operations, such as migration, backup, or consolidation. A collection of policies applicable to a particular managed store is called a policy set. Multiple policies of the same type may be defined in the same policy set.

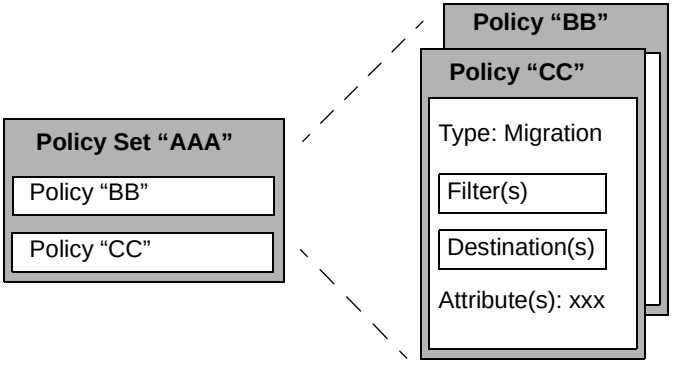
This release of Storage Migrator supports only migration policies. Multiple migration policies make it possible to migrate different sets of files to different stores.

Figure 6. Policy Sets



Each policy in a policy set may include one or more filters, must include one or more destinations, and may include some attributes specific to the policy type.

Figure 7. Policies



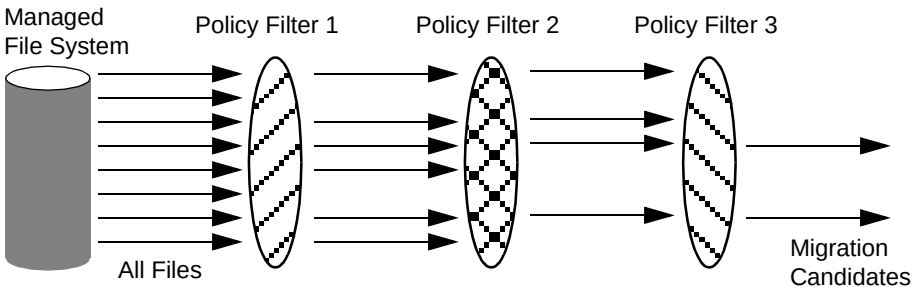
Filters

Filters define *which* files are subject to the policy.

By default, each policy applies to all of the files in the managed store. Restricting the policy to a particular subset of those files is done by one or more filters.

A policy only applies to files that match the file attributes specified in all of the selected and configured policy filters. In migration policies the filters include file size, time since last access or modification, and file type. See “Policy Attributes” on page 20 for more information. Also see “Filter Units of Measurement” on page 69.

Figure 8. Policy Filters



Destinations

Destinations define *where* the data from the files subject to the policy is copied.

Each policy defines a set of secondary stores to hold copies of the data selected by the policy. If multiple stores are listed in the destination, Storage Migrator will make multiple copies, one in each listed store. Storage Migrator does not support policies with the same source and destination store.

Attributes

Attributes vary from one policy type to another, and some policy types have no additional attributes. If a policy type contains additional attributes they must be specified. Defaults vary from attribute to attribute.

System Operations

Disk Full Conditions

Because Storage Migrator increases the amount of file space available to users by migrating files to secondary storage, the chances of encountering a Disk Full condition are greatly reduced. However, in circumstances when data is being written to disk faster than other data is being migrated and purged, the available free space diminishes and the file system can become completely filled. When this occurs, Storage Migrator blocks all further `write` operations to the full file system until the normal migration operations free additional space. Then the `write` operations resume automatically.

Disk Full conditions with Storage Migrator cause `write` operations to pause, but not to fail. No errors result. Performance may deteriorate because Storage Migrator blocks applications writing to disk, and staging delays may increase momentarily.

One way to reduce the number of Disk Full conditions you encounter is to tune your configuration by increasing the targeted free space. See “Modifying Migration Attributes in a File System” on page 42. Another way to do this is to schedule regular migration operations.

Scheduled Migrations

Migration activity to select files and copy the file data to secondary storage consumes resources which may impact overall system performance. You can avoid this performance impact during normal working hours by scheduling migration to occur outside of those hours.

See “Establishing a Regular Migration Schedule” on page 51 for more information.

System Backup

Migrating files is not a substitute for backup. Storage Migrator detaches the data from migrated files when they are purged from disk. This migrated data in secondary stores cannot be used to reconstruct the file paths and access modes of the original files. Use VERITAS NetBackup to back up each managed store, its databases, system registry, and local migration destination stores.

See “Backing Up a Managed Store” on page 52 for more information.

Disaster Recovery

In the unlikely event of a catastrophic failure involving the Storage Migrator system, it is possible to restore the system to the status it had prior to the last backup of the managed store, databases, system registry, and local migration destination stores.

See “Recovering from a Disaster” on page 53 for more information.

Configuring Storage Migrator Remote 2

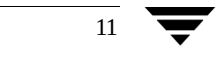
Configuring Storage Migrator using the administrator graphical user interface (Administration interface) is a quick and easy process. After selecting a file system to manage with Storage Migrator, you simply set a few migration attributes to manage the disk space in that file system. Then you apply a policy set to the file system that specifies which files will be migrated, how many copies will be migrated, and where those migrated copies will reside.

Administrator Interface (Administration Interface)

Bring up the Administration interface as follows:

1. On the task bar of your Windows NT desktop, click Start, and then point to Programs in the Start menu.
2. Point to VERITAS Storage Migrator in the Programs submenu, and then to the Administration icon.

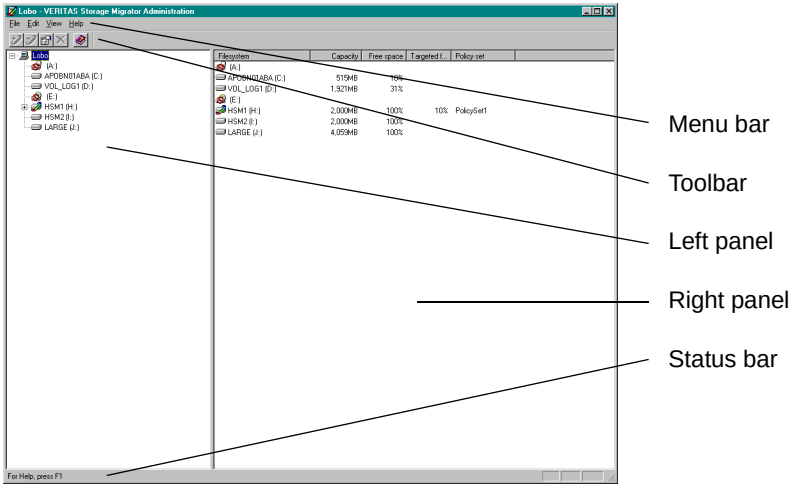
Note After a reboot, the Storage Migrator service may have to wait several minutes for the SQL server to initialize. If you attempt to bring up the Administration interface during that time, you will experience this delay. Once the SQL server has been initialized, however, the Storage Migrator service will start and the Administration interface will come up instantly.



Main Screen Layout

The main screen contains a menu bar, a toolbar, a status bar; and two panes, one on the left and one on the right.

Figure 9. Main Screen



Menu Bar

The menu bar consists of four drop-down menus:

File

- Use the File menu to exit the program.

Edit

- Use the Edit menu to manage or unmanage the selected file system, show the properties of the selected item, or delete the selected item.

View

- Use the View menu to display or to hide the toolbar or status bar.

Help

- Use the Help menu to open the online Help window.

Toolbar

The toolbar consists of five tool elements that duplicate the more frequently used commands in the menu bar.

Manage

Click the Manage tool to manage the selected unmanaged file system.

Unmanage

Click the Unmanage tool to unmanage the selected managed file system.

Properties

Click the Properties tool to show the properties of the selected item.

Delete

Click the Delete tool to delete the selected item.

Help

Click the Help tool to open the online Help window.

Status Bar

The status bar at the bottom of the window provides general information about this interface.

Left Pane

The main screen displays a tree structure of the Storage Migrator Server and its file system(s) in the Pane on the left of the window.

- To expand or collapse the information displayed in this Pane, click selected nodes in the tree.

Right Pane

When you select a particular element in the left (tree) Pane, the Pane on the right of the window displays information about that element.

Configuration Process

Configuring Storage Migrator is a simple process using the Administration interface.

1. Select a File System to Manage.
2. Set Migration Attributes.
3. Apply a Policy Set.
4. Select Another File System to Manage (optional).

Select a File System to Manage

Expand the Storage Migrator Server icon to reveal the file systems loaded on the server. Each file system is a primary store. Once a file system is selected and configured it becomes a managed store.

Note You cannot manage the System folder. You cannot migrate the Windows NT Registry, the Storage Migrator database, nor any Storage Migrator executables.

Figure 10. File System Structure on Storage Migrator Server

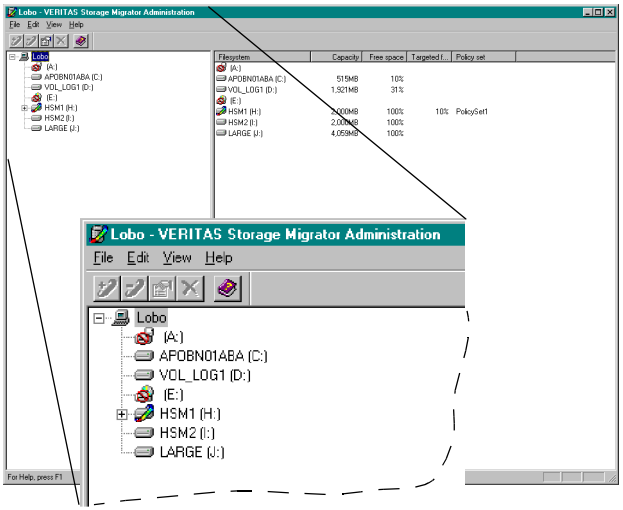


Table 1. File System Icons

Icon	Icon Description
	**Manageable File System:** an unmanaged file system that could be managed by Storage Migrator
	**Managed File System:** a file system managed by Storage Migrator
	**Previously Managed File System:** a file system that is no longer managed by Storage Migrator, but on which migrated files can still be staged
	**Unmanageable File System:** a file system that can not be managed by Storage Migrator

Note See Table 2 on page 31 for a complete list of Storage Migrator icons.

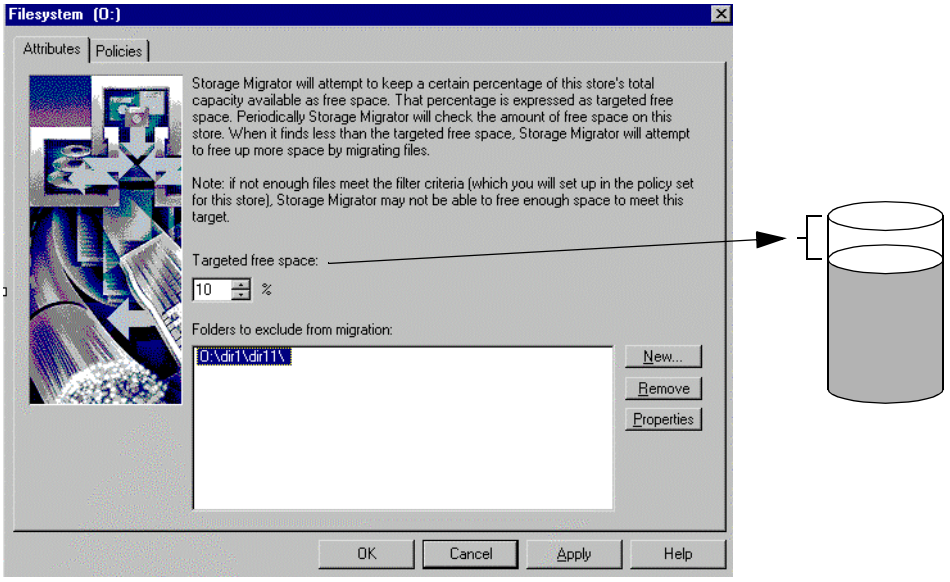
Select a manageable file system to manage with Storage Migrator, and click the Manage tool in the toolbar.

Set Migration Attributes

The File System Attributes dialog shows two migration attributes:

- The Targeted free space field determines how Storage Migrator will manage the disk space in the managed store.
- The Folders to exlude from migration field allows you to select directories that Storage Migrator will not manage (see Figure 11).

Figure 11. File System Attributes Dialog



Targeted free space

Targeted free space is the amount of file system capacity on disk that Storage Manager tries to keep available for use. It is expressed as a percent of total file space. The default is 10 percent.

In the Targeted free space box, type in a new value or click the arrows to select a new value. Click OK.

Folders to exclude from migration

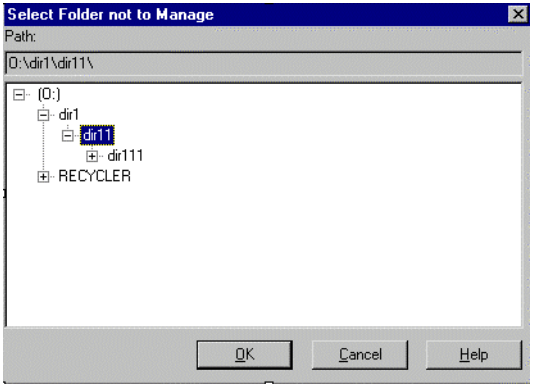
Folders to exclude from migration allows you to prevent Storage Migrator from migrating files in folders.

Note Selecting Folders to exclude from migration does not override the policy filters. See "Policy Filters" on page 21.

- To remove a folder from the excluded folder list, select that folder and click Remove (see Figure 11). Then click OK.
- To view the properties of a folder displayed in this field, select that folder and click Properties (see Figure 11). Then click OK.
- To exclude a folder from migration (*not* manage a folder with Storage Migrator), click New on the File System Attributes dialog. You will then see the Select Folder not to Manage dialog (see Figure 12). Select the directory you wish to exclude and click OK.

  This will return you to the File System Attributes dialog. Then click OK. Repeat this process for each folder you want to exclude from migration.

Figure 12. Select Folder not to Manage Dialog

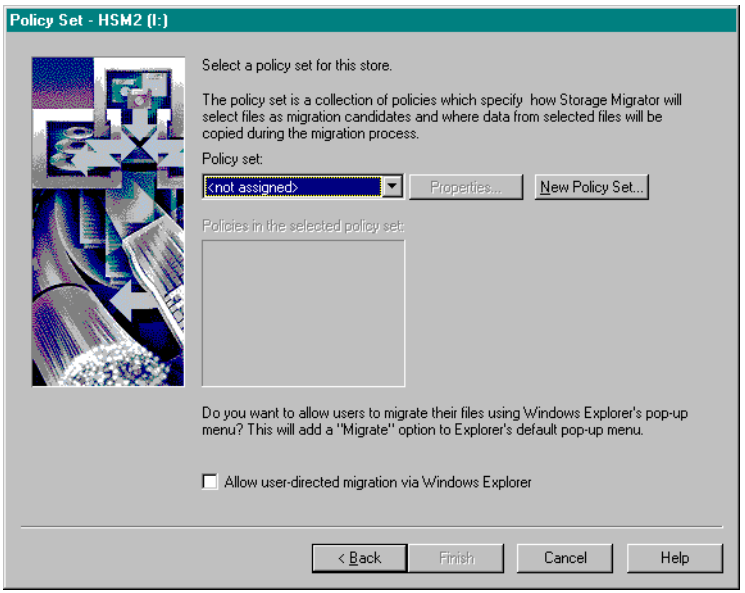


When you are satisfied with the configuration of these migration attributes, click Apply. The Policy Set dialog appears.

Apply a Policy Set

The policy set determines the exact operations Storage Migrator performs on the managed store. It specifies how Storage Migrator will select files as migration candidates and where data from the selected files will be copied during the migration process. See Figure 13 on page 18.

Figure 13. Policy Set Dialog



Apply a policy set to a file system by selecting an existing policy set or by creating a new policy set.

Existing Policy Set

If you select an existing policy set from the drop-down list and insert it in the Policy set field, click Finish to apply this policy set to the managed store (see Figure 13). Then, go to Figure 26 on page 31.

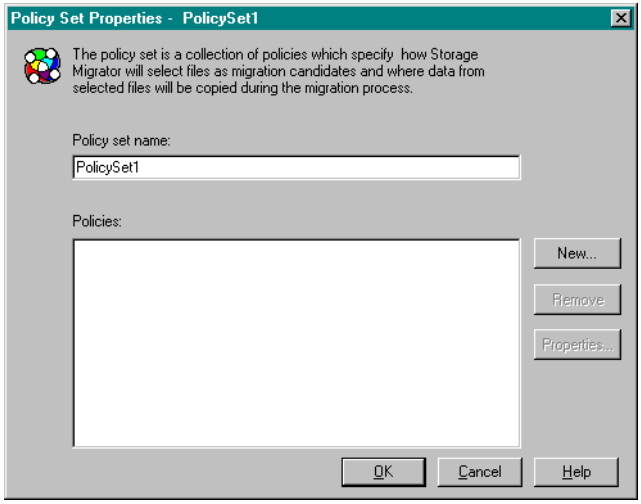
New Policy Set

If you click New policy set, the Policy Set Properties dialog appears (see Figure 14).

Enable User Migration

Select the check-box to allow end-users to migrate their files using Windows Explorer. If not selected, this option is unavailable to users (see Figure 14). Then, see “Using Storage Migrator Remote” on page 57.

Figure 14. Policy Set Properties



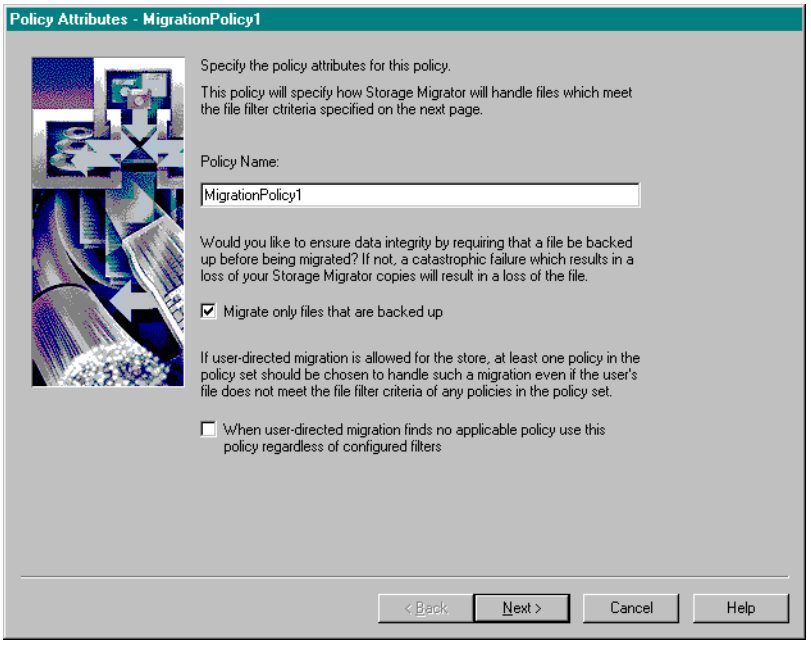
Type the name of the new policy set in the Policy set name field, or accept the name provided.

Note Policy set names configured for Storage Migrator must be unique.

Add a New Policy

Click New to add a new policy to the policy set (see Figure 14).

Figure 15. Policy Attributes Dialog



Policy Attributes

Type the name of the new policy in the Policy name field, or accept the name provided (see Figure 15). Policy names in a policy set must be unique.

Select the first check box, Migrate only files that are backed up, in each migration policy (default). This is necessary to ensure migration data integrity when recovering from a catastrophic failure involving the Storage Migrator system. If you decide to clear this check box, you must configure a filter in this migration policy to make sure no changed files will be migrated before they are backed up at least once. See “Recovering from a Disaster” on page 53.

Select the second check-box, When user-directed migration finds no applicable policy..., for at least one migration policy if user-directed migration is allowed on the Store Attributes dialog. See Figure 13 on page 18. If selected and the file does not meet the filter criteria of any policy in this policy set, a user-directed forced migration will be migrated to the stores configured for the selected policy regardless of filter criteria. If not selected for any migration policy (default), a user-directed forced migration will fail if the file does not meet the filter criteria of any policy in this policy set.

Set Migration Criteria

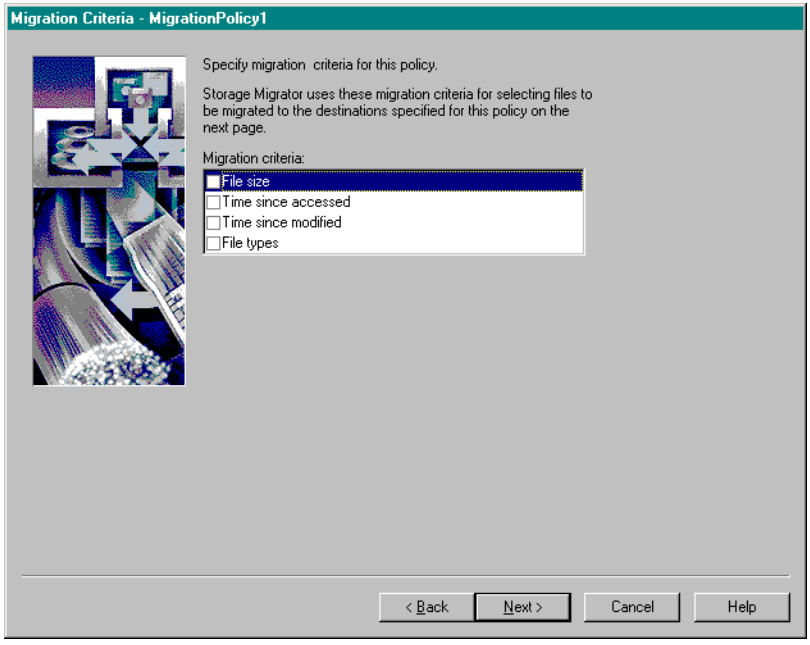
Click Next, and the Migration Criteria dialog appears (see Figure 16).

Policy Filters

This dialog defines *which* files are subject to the policy. A policy only applies to files that match all of the file filters specified in this dialog.

- In the initial (default) display of this dialog, none of the four file attributes apply and all files are subject to the policy. To configure a particular file attribute filter, select its check box and fill in the fields with your desired settings.
- To disregard a configured file attribute filter, clear its check box. This collapses the configurable fields and the policy no longer filters on this file attribute after you commit the revised policy.

Figure 16. Migration Criteria Dialog

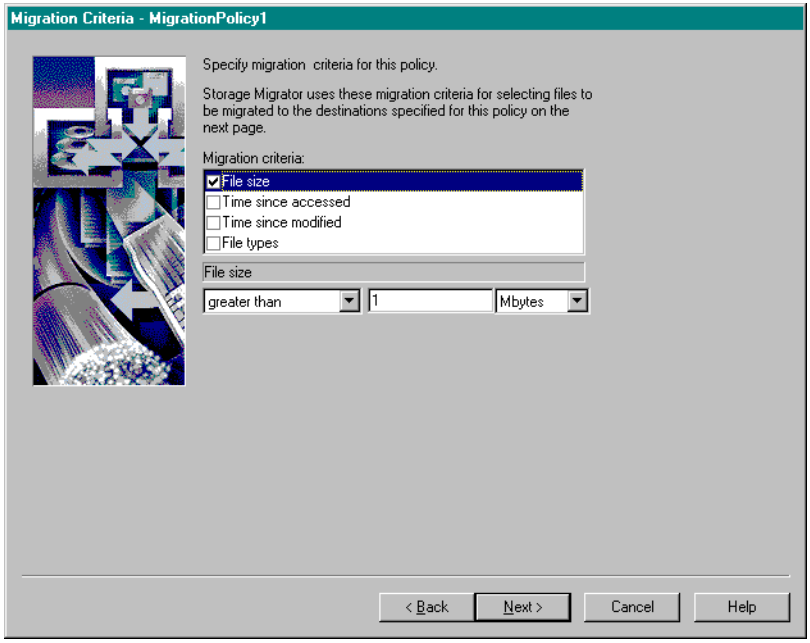


Attribute values for size or time are specified as an operator, number, and unit. See “Filter Units of Measurement” on page 69 for a detailed description of each size and time unit.

File Size

Consider only those files that match the configured criteria for file size. Complete the operator, number, and unit fields. Decimal values are recognized. If no file size is specified, consider files of any size. (see Figure 17).

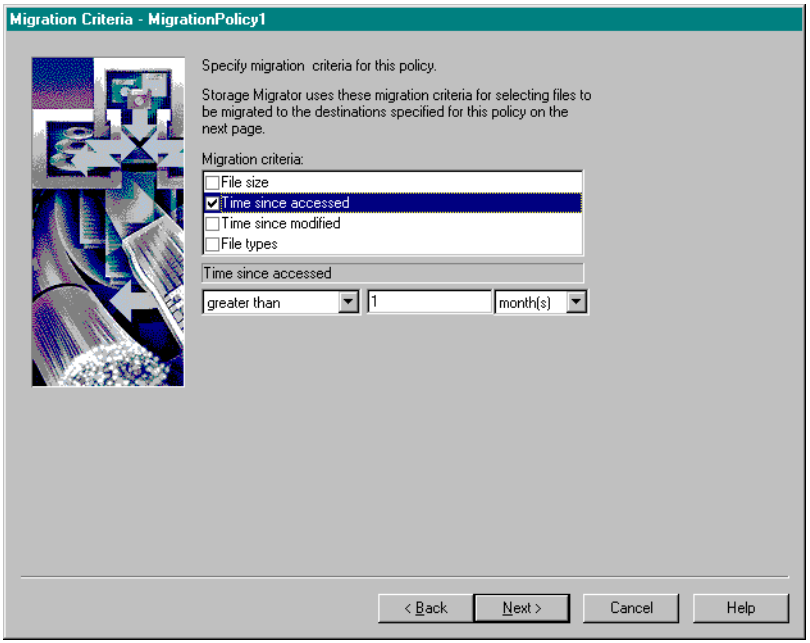
Figure 17. Migration Criteria Dialog, File Size



Time Since Accessed

Consider only those files that match the configured criteria for file age since last access. Complete the operator, number, and unit fields. Decimal values are recognized. If no age is specified, consider files without regard to time since last access (see Figure 18).

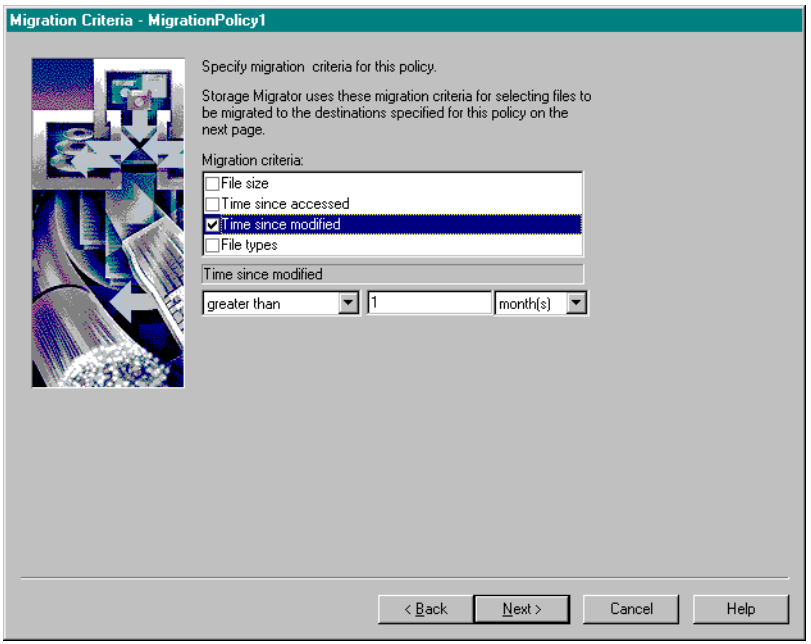
Figure 18. Migration Criteria Dialog, Time Since Accessed



Time Since Modified

Consider only those files that match the configured criteria for file age since last modification. Complete the operator, number, and unit fields. Decimal values are recognized. If no age is specified, consider files without regard to time since last modification. (See Figure 19.)

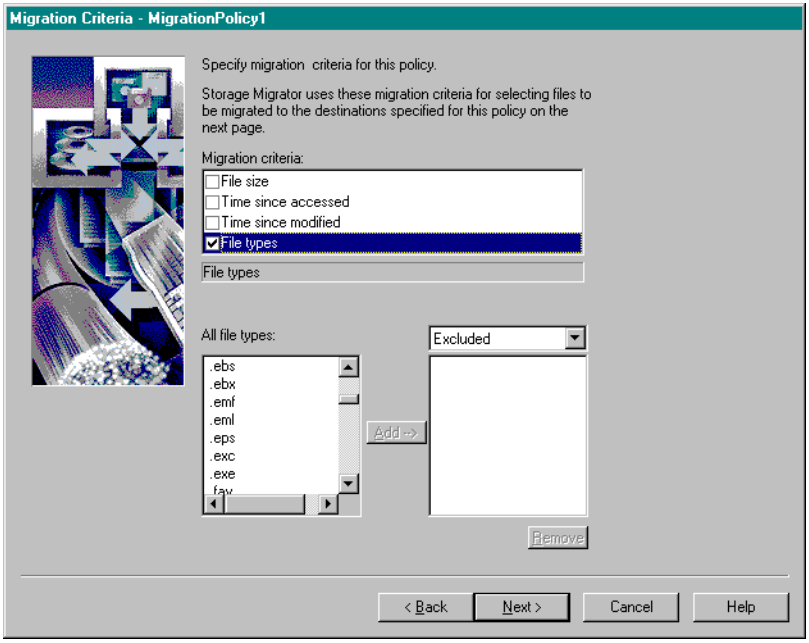
Figure 19. Migration Criteria Dialog, Time Since Modified



File Types

Consider only those files whose file types (extensions) are in the selected Included list *or* are not included in the selected Excluded list. If the Excluded list is empty, consider files of any file type. (See Figure 20.)

Figure 20. Migration Criteria Dialog, File Types



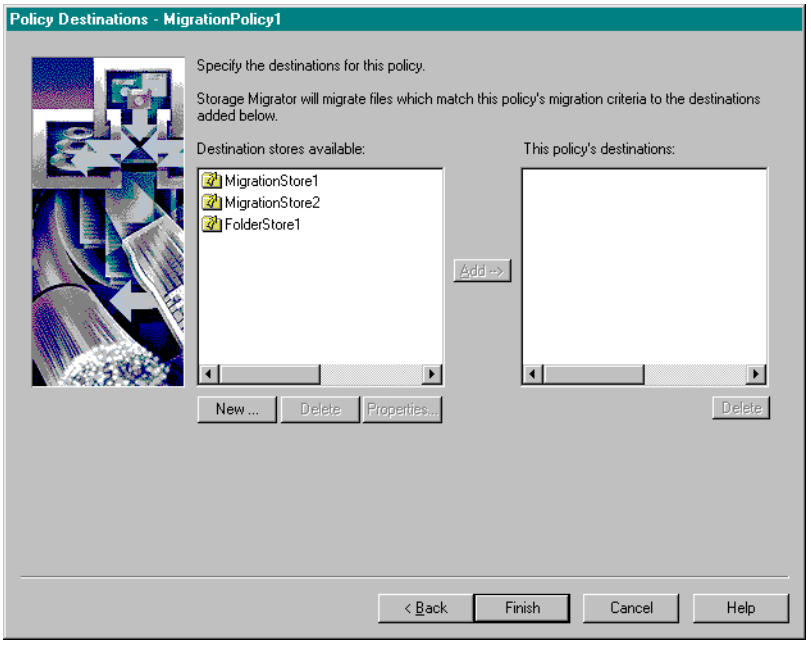
Remember, a policy only applies to files that match *all* of the file attributes specified in this dialog. If none of the filter check boxes are selected, none of the four file attributes apply and all files are subject to the policy.

Click Next, and the Policy Destinations dialog appears. (See Figure 21.)

Policy Destinations Dialog, Phase 1

Policy Destinations

Figure 21. Policy Destinations Dialog, No Stores Configured

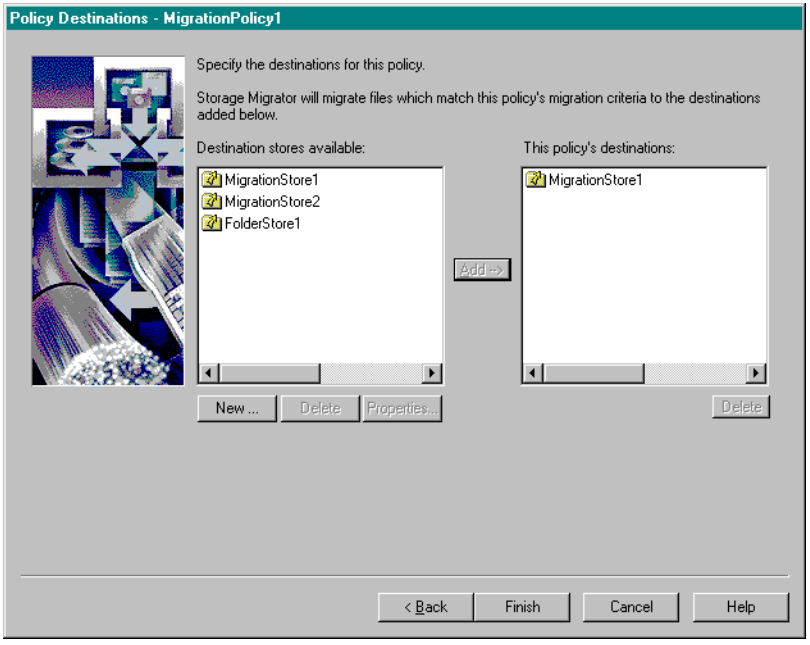


This dialog defines *where* files subject to the policy are copied. An active policy requires at least one destination store. If you select multiple destination stores, Storage Migrator will make multiple copies, one in each listed destination store.

Note Making multiple migration copies means you are more certain to recover migrated data in case of a system failure.

- To configure an existing destination store, select one from the list of Destination stores available and move it to the list of This policy's destinations using the Add button.

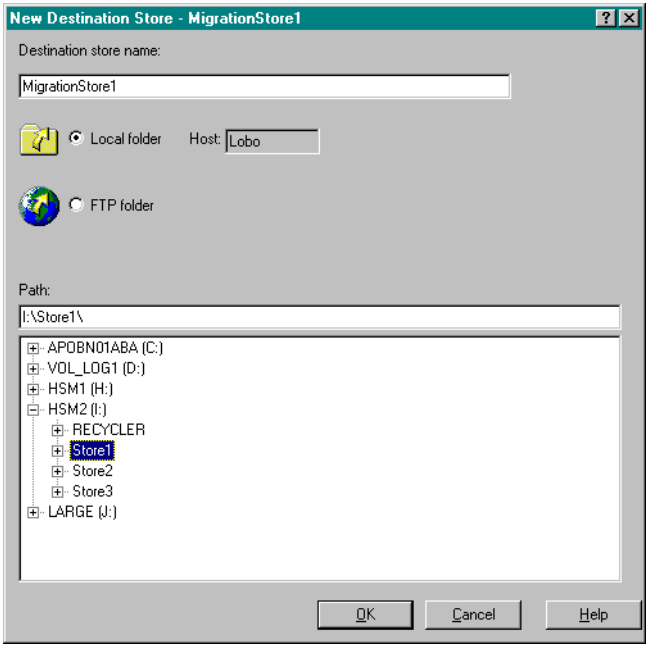
Figure 22. Policy Destinations Dialog, One Store Configured



- To create a new store and add it to the list of This policy's destinations, click New. The New Destination Store dialog appears.

New Destination Store

Figure 23. New Destination Store Dialog, Local Folder



Type the name of the new destination store in the Destination store name field, or accept the name provided. Store names configured for Storage Migrator must be unique.

Select either Local folder on Host, or FTP folder.

Local Folder on Host

Expand or collapse the information displayed in the Pane by clicking on selected nodes in the tree. Select one of the available folder stores. Click OK.

Destination store name: the name of the folder store.

Host: the name of the Storage Migrator domain.

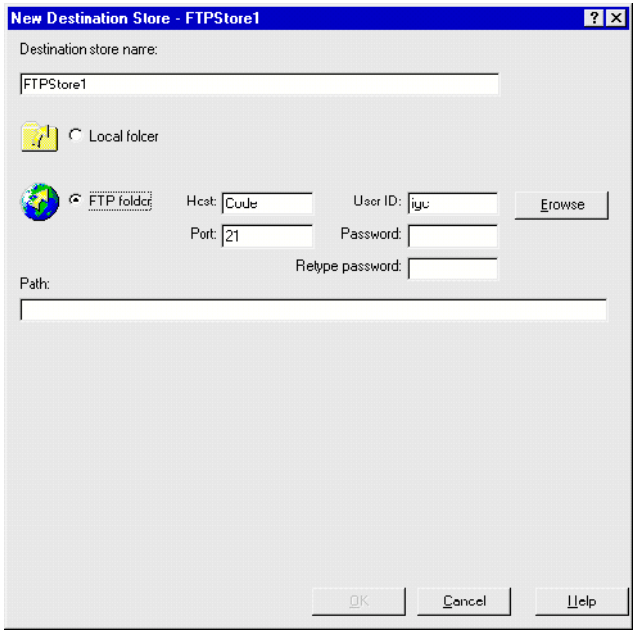
Path: the path to the folder store.

Note You cannot select the System folder as a secondary store.

FTP Folder

Note See “Configuring a Remote Destination Store” on page 50 for information on how configure the server to recognize a remote destination for FTP transmissions.

Figure 24. New Destination Store Dialog, FTP Folder



Destination store name: the name of the folder store

Host: the name of the FTP server

Port: the number of the FTP port

User ID: the configured user identifier

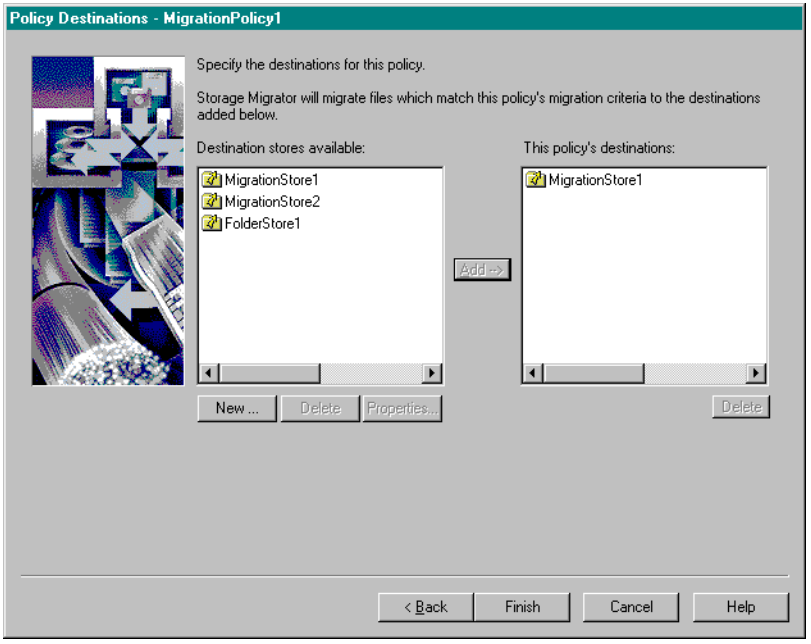
Password: the configured password of the user

Path: the path to the FTP store on the FTP server

When you complete the New Destination Store dialog, click OK. This returns you to the Policy Destinations dialog (see Figure 25).

Policy Destinations Dialog, Phase 2

Figure 25. Policy Destinations Dialog, One Store Configured



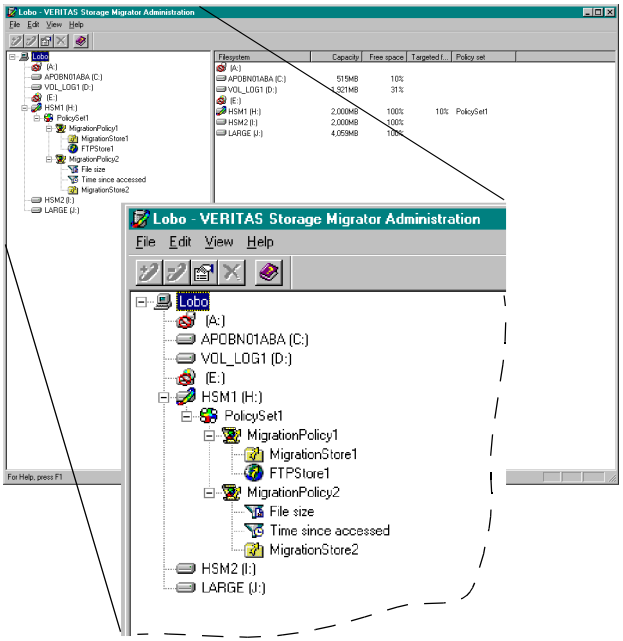
Wrap-up

When you have configured the desired number of destination stores and otherwise completed the Policy Filters and Policy Destinations dialogs, click Finish. This returns you to the Policy Set Properties dialog.

Multiple policies of the same type may be defined in the same policy set. Multiple migration policies make it possible to migrate different sets of files to different stores. If you want to add another policy to this policy set, go to “Add a New Policy” on page 19 and repeat this procedure.

When you have included the desired number of policies in the policy set, accept all open dialogs and return to the main screen to apply this policy set to the managed store.

Figure 26. Managed File System Structure on Storage Migrator Server



The left Pane of the main screen can display not only a tree structure of the Storage Migrator Server and its file system(s), but also the policy set, migration policies, filters, and destination stores configured for any managed file system.

These are the icons for the managed and unmanaged elements as displayed in the tree in the left Pane.

Table 2. Storage Migrator Icons

Icon	Icon Description
	**Managed File System:** a file system managed by Storage Migrator
	**Previously Managed File System:** a file system that is no longer managed by Storage Migrator, but on which migrated files can still be staged
	**Unmanageable File System:** a file system that can not be managed by Storage Migrator

Icon	Icon Description
	**Unmanageable CD-ROM Drive:** a CD-ROM drive that can not be managed by Storage Migrator
	**Unmanageable Floppy Disk Drive:** a floppy disk drive that can not be managed by Storage Migrator
	**Policy Set:** a collection of policies applicable to a particular managed store
	**Migration Policy:** the configurable specifications that define the exact operations Storage Migrator performs on a managed store
	**Migration Filter:** that part of a migration policy which defines which files are subject to the policy
	**File Size Filter:** a migration filter with configured criteria for file size
	**Time Since Accessed Filter:** a migration filter with configured criteria for the time since files were last accessed
	**Time Since Modified Filter:** a migration filter with configured criteria for the time since files were last modified
	**File Type Filter:** a migration filter with configured criteria for file type
	**Local Store:** a folder local to the Storage Migrator Server
	**FTP Store:** a folder on a remote Windows NT system that is shared to the Storage Migrator server

Icon	Icon Description
	**Connection Broken:** displayed under a node that can not be expanded because the connection is broken

Select Another File System to Manage (optional)

Storage Migrator can manage several different file systems on a single Storage Migrator Server. To do this, simply repeat the same configuration procedure for each file system you intend to manage. See “Select a File System to Manage” on page 14.

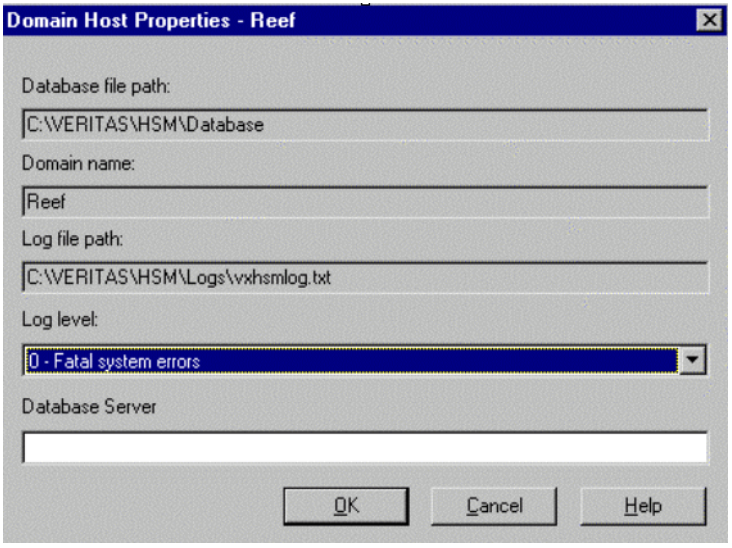
Element Properties

After you have configured Storage Migrator Remote, you can easily review the properties of any element in the hierarchy by selecting it and clicking the Properties tool in the toolbar.

Domain Host Properties

On the left pane of the main screen, right-click the domain host icon and choose Properties (see Figure 27).

Figure 27. Domain Host Properties



Data file path: the location of the SQL Server database files used by Storage Migrator.

Domain name: the name of the Storage Migrator domain (your host).

Log file path: the location of the log file maintained by Storage Migrator.

Log level: the numerical level (0-9) for sorting log messages. Default is 0.

You can change the parameters in this field. It determines which messages are written into the specified log file.

Higher log levels cause more detailed messages to be written. By default, only fatal system errors are written to the log file. Higher level messages are used for problem analysis by VERITAS Customer Support personnel.

Do not increase Log level unnecessarily, because the log file is not recycled by the system. You can manually remove or truncate the log file if necessary.

Database server: an alternate database server you may use to run VSM in a Microsoft Cluster Server (MSCS) environment. This field is blank when VSM is connected to the local database (shown in Figure 27 on page 34). This field lists the name of your failover server if the local database fails and VSM is configured as a cluster server.

Note You can change the parameters in this field. However, if you connect to a different database server, all migrated files on the previous database are no longer accessible to you.

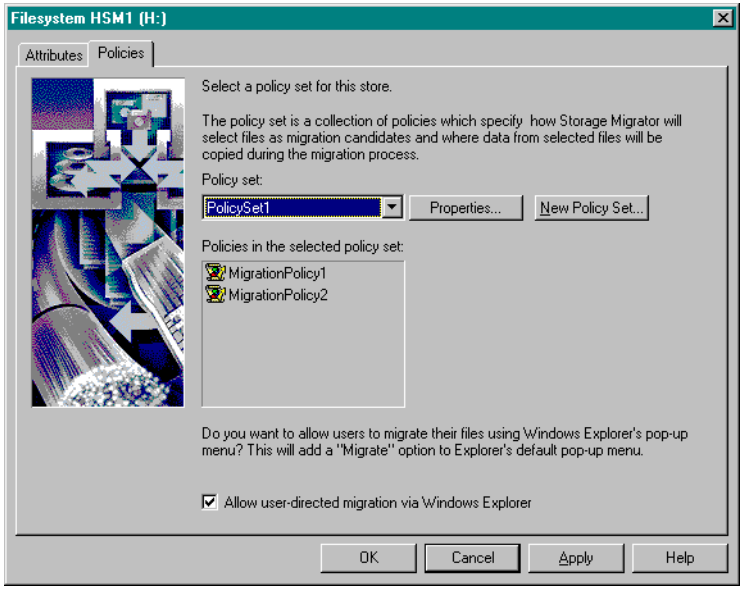
File System Properties

On the left pane of the main screen, right-click a file system icon and choose Properties. The File System properties dialog contains two tabbed categories: Attributes and Policies.

The Attributes tab shows the configured Targeted Free Space and Migration Preference attributes for this managed store. See “Set Migration Attributes” on page 16.

The Policies tab identifies the policy set for this managed store, and shows the policies contained in the policy set. See “Apply a Policy Set” on page 17.

Figure 28. File System Properties

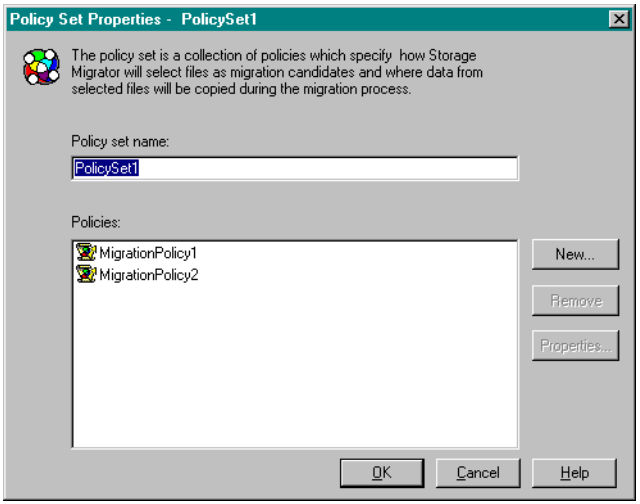


Policy Set Properties

On the left pane of the main screen, right-click a policy set icon and choose Properties.

The Policy Set Properties dialog identifies the policy set for this managed store, and shows the policies contained in the policy set (see Figure 29).

Figure 29. Policy Set Properties



Policy Properties

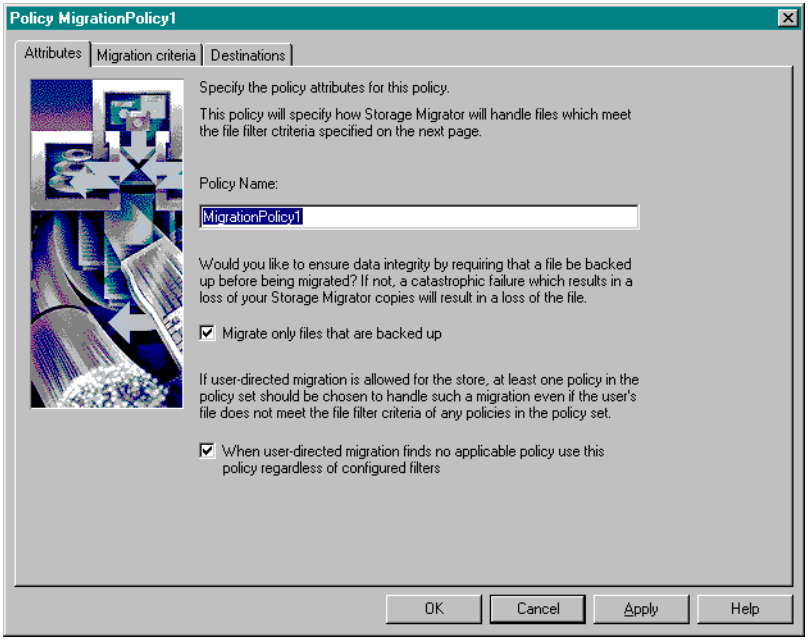
On the left pane of the main screen, right-click a policy icon and choose Properties. The Policy properties dialog contains three tabbed categories: Attributes, Migration Criteria, and Destinations (see Figure 30).

The Attributes tab shows the configured Targeted Free Space and Migration Preference attributes for this managed store. See “Set Migration Attributes” on page 16.

The Migration Criteria tab shows the filter properties of this policy. See “Filter Properties” on page 38.

The Destinations tab shows the destination stores configured for this policy. See “Filter Properties” on page 38.

Figure 30. Policy Properties

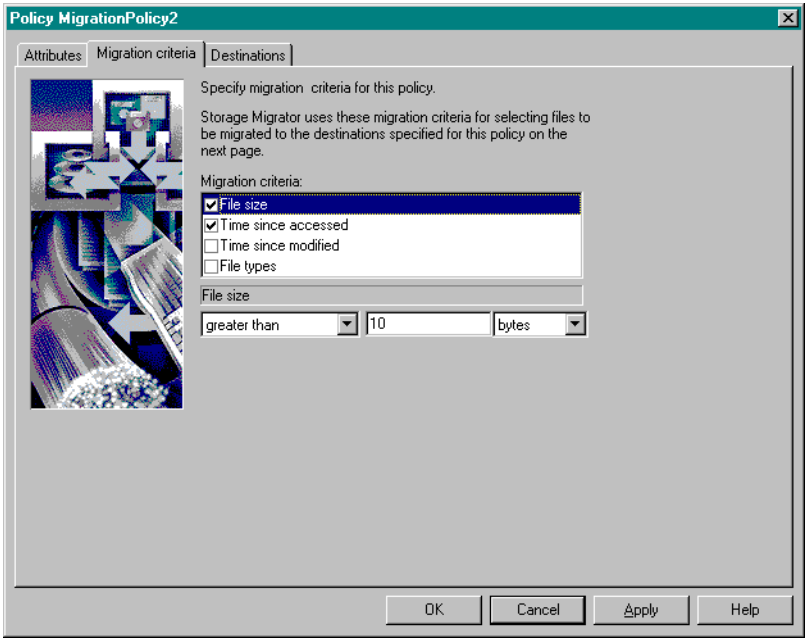


Filter Properties

On the left pane of the main screen, right-click a filter icon and choose Properties. The Migration Criteria tab of the Policy properties dialog shows the filter properties for this policy (see Figure 31).

A policy only applies to files that match *all* of the file attributes specified in this dialog. If none of the filter check boxes are selected, none of the four file attributes apply and all files are subject to the policy.

Figure 31. Filter Properties



Folder Store Properties

On the left pane of the main screen, right-click a folder store icon and choose Properties (see Figure 32).

Figure 32. Local Store Properties

Store name: the name of the folder store. You can rename a folder store, if desired.

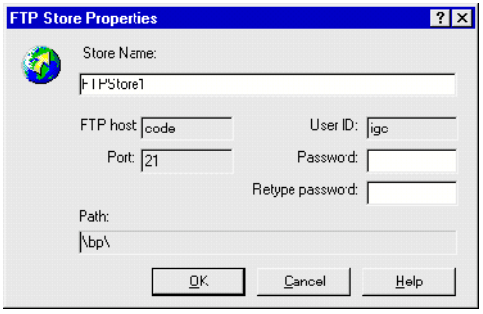
Host: the name of the Storage Migrator domain.

Path: the path to the folder store. You cannot change the path because it would cause you to lose access to your migrated data.

FTP Store Properties

On the left pane of the main screen, right-click an FTP store icon and choose Properties (see Figure 33).

Figure 33. FTP Store Properties



Store name: the name of the FTP store. You can rename an FTP store, if desired.

FTP host: the name of the FTP server you upgraded.

Port: the number of the FTP port.

User ID: the configured user identifier.

Password: the configured password of the user. You can change a password to reflect password changes on the FTP server.

Path: the path to the FTP store on the FTP server. You cannot change the path because it would cause you to lose access to your migrated data.

Managing Storage Migrator Remote 3

Once you have been operating Storage Migrator in production mode to manage file space on one or more file systems, you may modify the configuration at any time to administer or manage your file space more effectively.

Initial configuration and subsequent reconfiguration are possible in real time without stopping Storage Migrator. As soon as a policy is configured it becomes operational, and data migration occurs in accordance with the cumulative effect of *all* active policies.

Reconfiguration Procedures

- Modifying Migration Attributes in a File System
- Modifying the Filter in an Existing Policy
- Adding a Store to an Existing Policy
- Adding a New Policy to a Policy Set
- Reusing an Existing Policy Set
- Removing a Policy Set from a Managed Store

Configuration Procedures

- Configuring a Remote Destination Store

Management Procedures

- Establishing a Regular Migration Schedule
- Backing Up a Managed Store
- Recovering from a Disaster

Modifying Migration Attributes in a File System

This procedure shows how to change migration attributes in a managed file system while Storage Migrator is running.

Example Situation

Your policy set has the Targeted free space attribute set at 2 percent. This leaves only a very small amount of file space unused in the managed file system, and you experience deteriorating performance. Each time the system encounters a Disk Full condition, Storage Migrator blocks applications writing to disk, and staging delays may increase momentarily. You decide to change the Targeted free space attribute from 2 percent to 10 percent to increase the nominal amount of file space on disk that is not utilized.

Resulting Action

Storage Migrator will begin purging previously migrated files whenever the available free space drops below 10 percent. This immediately increases the nominal disk free space to ten percent of the managed file system, enabling more files to be written to disk without reaching a Disk Full condition.

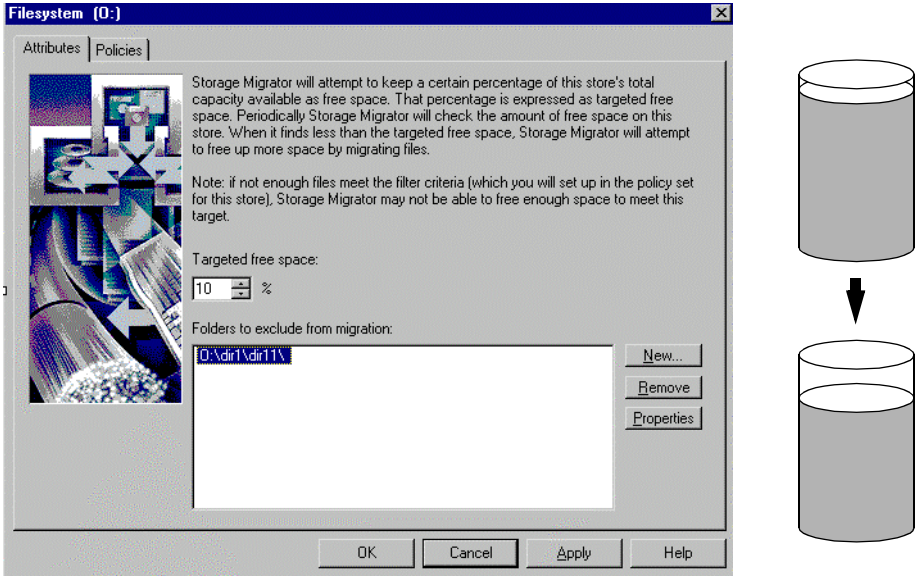
Procedure

1. Right-click the icon of the managed file system, and select Properties from the pop-up menu.

   On the File Systems properties dialog, select the Attributes tab.

2. In the Targeted free space box, type in 10 or click the arrows to read 10 percent. See “Set Migration Attributes” on page 16.

Figure 34. File System Properties Dialog, Change Targeted Free Space



3. Click OK to return to the main screen. The change is implemented automatically.

Modifying the Filter in an Existing Policy

This procedure shows how to change the filter in an existing policy while Storage Migrator is running.

Example Situation

Your configured policy set contains one migration policy with the file size configured to be greater than or equal to 20 kilobytes. You find that your managed file system fills up with files smaller than 20 kilobytes, and you want to migrate more files. You decide to modify the policy filter and reduce the minimum file size from 20 to 8 kilobytes.

Resulting Action

Storage Migrator will begin considering for migration those files that meet or exceed 8 kilobytes. All other configured filter conditions for this policy must also be met.

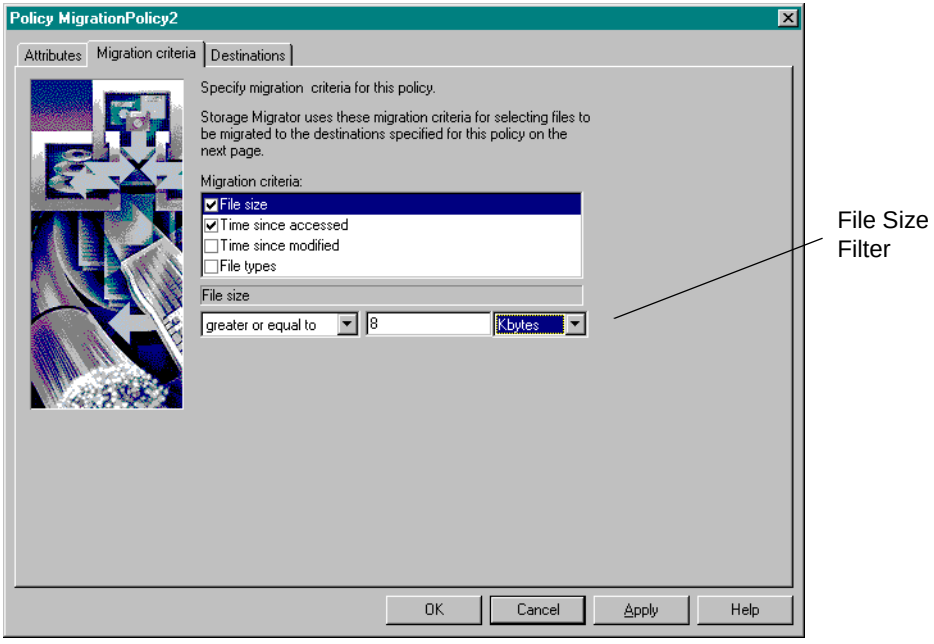
Note If the minimum size is increased, all files previously migrated stay migrated until cached, regardless of size. If a cached file is modified it will not be migrated again if it falls below the new minimum size.

Procedure

1. Right-click the icon of the migration policy you want to modify, and select Properties from the pop-up menu.
2. On the Policy properties dialog, select the Filters tab, and make sure the File size check box is checked.
3. Change theFile size filter to read:

```
greater or equal to 8 Kbytes
```

Figure 35. Policy Properties Dialog, Change File Size



4. Click OK to return to the main screen. The change is implemented automatically.

Adding a Store to an Existing Policy

This procedure shows how to add another destination store to existing policy while Storage Migrator is running.

Example Situation

Your configured policy set contains one migration policy with a single configured destination, `MigrationStore1`. Storage Migrator copies migrated data once to `MigrationStore1`. To improve the robustness of disaster recovery for your system, you decide to add a second destination, `MigrationStore2`, to the policy.

Resulting Action

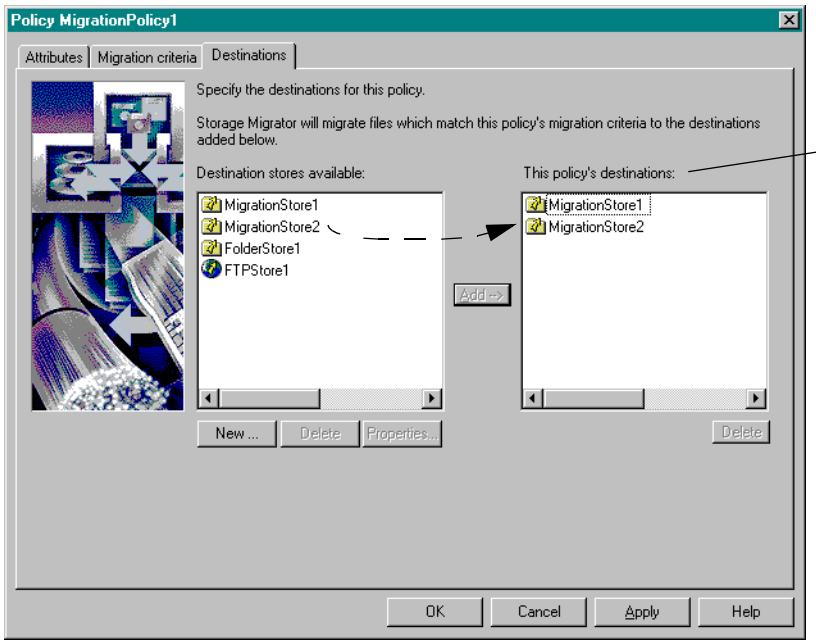
Storage Migrator will begin making two copies of migrated data, one copy to `MigrationStore1` and another copy to `MigrationStore2`.

Note The next time Storage Migrator considers a file previously migrated only to `MigrationStore1` it will migrate a second copy to `MigrationStore2`. This action may not occur immediately because it is a function of the internal sweeping process, which is affected by the size of the entire managed file system.

Procedure

1. Right-click the icon of the migration policy you want to modify, and select Properties from the pop-up menu.
2. On the Policy properties dialog, select the Destinations tab.
3. If `MigrationStore2` is an existing store, select it from Destination stores available and move it to This policy's destinations using the Add button.

Figure 36. Policy Properties Dialog, Add Another Destination



4. If `MigrationStore2` is not an existing store, create a new store and add it to the list by clicking New. The New Destination Store dialog appears. When you complete the New Destination Store dialog, click OK. This returns you to the Policy dialog.

5. When `MigrationStore2` appears in This policy's destinations, accept all open dialogs and return to the main screen. The change is implemented automatically.

Adding a New Policy to a Policy Set

This procedure shows how to add another policy to existing policy set while Storage Migrator is running.

Example Situation

Your configured policy set contains one migration policy that migrates files of type (extension) `.doc` to `MigrationStore1`. No files of type `.xls` are migrated, and they remain in the managed file system. You decide to add a second policy that will migrate files of type `.xls` to `MigrationStore2`.

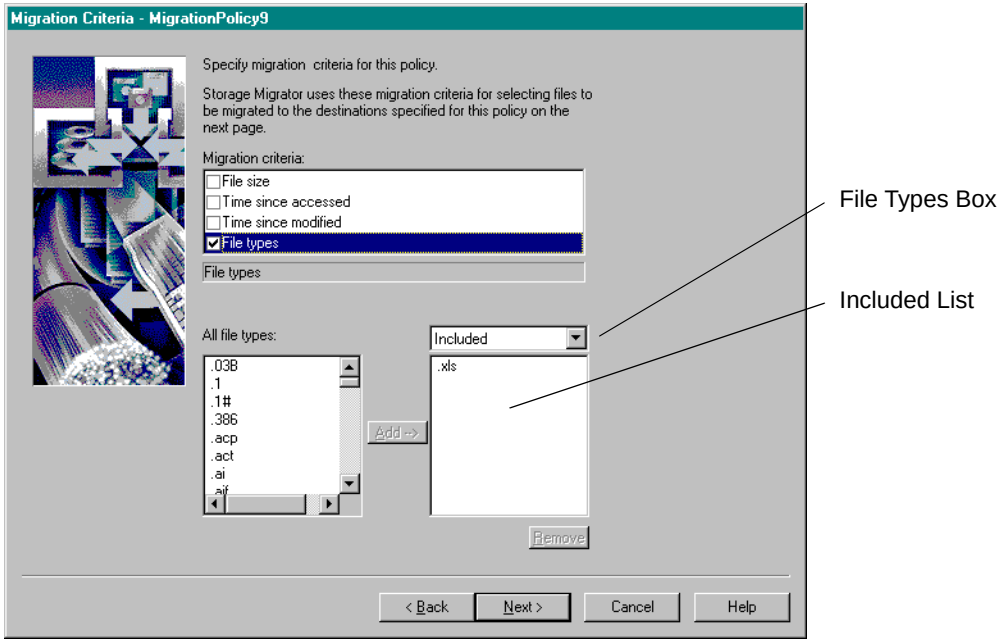
Resulting Action

Storage Migrator will begin considering for migration those files of type `.xls`, and copy the migrated data to `MigrationStore2`. All other configured filter conditions for this policy must also be met. Files of type `.doc` will continue to be migrated to `MigrationStore1` as before.

Procedure

1. Right-click the icon of the policy set for your `.doc` and `.xls` files, and select Properties from the pop-up menu.
2. On the Policy Set Properties dialog, click New. The Policy Attributes dialog appears.
3. Type the name of the new policy in the Policy name field, or accept the name provided. Policy names in a policy set must be unique. Click Next, and the Migration Criteria dialog appears.
4. Click the File types check box, and select the Included list of file types from the drop-down File types box.
5. Remove all file types except `.xls` from the Included list by using the Remove button.

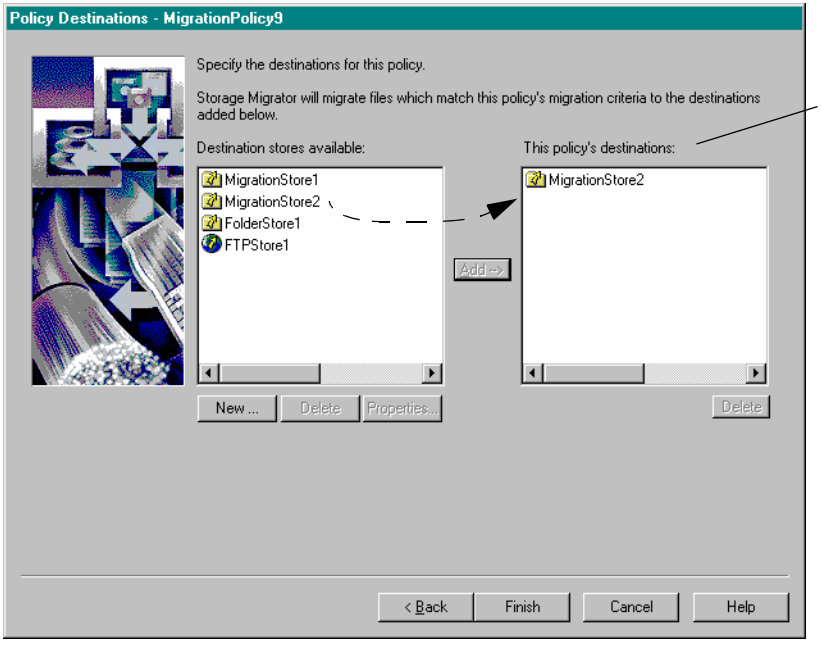
Figure 37. Set Up Filters Dialog, New Filter



6. Click Next, and the Policy Destinations dialog appears.

7. If `MigrationStore2` is an existing store, select it from Destination stores available and move it to This policy's destinations using the Add button.

Figure 38. Policy Dialog, Specify a Destination



8. If `MigrationStore2` is not an existing store, create a new store and add it to the list by clicking New. The New Destination Store dialog appears. When you complete the New Destination Store dialog, click OK. This returns you to the Policy Destinations dialog.

9. When `MigrationStore2` appears in This policy's destinations, click Finish and return to the main screen. The change is implemented automatically.

Reusing an Existing Policy Set

This procedure shows how to apply an existing policy set to another file system while Storage Migrator is running.

Example Situation

You have two managed file systems, where `policyset_A` applies to `filesystem_A`, and `policyset_B` applies to `filesystem_B`. You want to start managing a third file system, `filesystem_C`, by applying one of your existing policy sets instead of configuring a totally new policy set. You decide to reuse `policyset_A`.

Resulting Action

Storage Migrator will apply the same migration policies to `filesystem_C` that it applies to `filesystem_A`. The migration attributes (Targeted free space and Migration preference) do not need to be the same in `filesystem_A` and `filesystem_C`.

Procedure

1. Right-click the icon of `filesystem_C`, and select Manage from the pop-up menu.
2. Set the two migration attributes on the File System Attributes dialog to their desired values. See “Set Migration Attributes” on page 16. Click Next. The Policy Set dialog appears.
3. Select `policyset_A` from the drop-down list, and click Finish to return to the main screen. The change is implemented automatically.

Removing a Policy Set from a Managed Store

This procedure shows how to remove an existing policy set from a managed store while Storage Migrator is running. This interrupts file migration from that managed store.

Example Situation

You have several managed file systems. One of these, `filesystem_old`, is no longer heavily used. You decide to stop migrating files from `filesystem_old` by removing the policy set applied to it. The policy set is named `policyset_old`.

Resulting Action

Storage Migrator stops managing `filesystem_old` and migrating files to secondary stores. All files previously migrated remain migrated, and will be staged if accessed. Staged files, however, will not be re-migrated if modified.

Caution You must leave Storage Migrator installed to allow access to migrated data.

Procedure

1. Select `filesystem_old`.
2. Click the Unmanage tool in the toolbar.

Configuring a Remote Destination Store

This procedure shows how to configure a folder on a remote FTP server and configure it as a destination store.

Example Situation

You have some special project files you want Storage Migrator to migrate to a remote destination store using File Transfer Protocol (FTP).

- If the remote FTP server is an Windows NT server, you first must configure an FTP folder on that server for storing these special project files.
- If the remote FTP server is a UNIX server, you only need to identify which directory you will use as an FTP folder.

In either case, you add the FTP folder to This policy's destinations for the policy you will use to select and migrate these special project files.

Resulting Action

Storage Migrator will select and migrate your special project files to the remote FTP folder.

Procedure

If you are configuring an FTP store on an remote Windows NT server, complete the following:

1. On the taskbar of the Windows NT desktop on the server, click Start, and then point to Programs in the Start menu.
2. Point to Microsoft Internet Server (Common) in the Programs submenu.
3. Use Internet Service Manager to get the FTP Services Properties window.
4. Configure the FTP folder as the FTP service home directory or under the FTP service home directory.
5. Give the FTP folder on the FTP server both Write and Read permission to enable file migration and file staging.

If you are configuring an FTP store on a remote UNIX platform, complete the following:

- On Storage Migrator, create a new policy that filters the special project files, and add the new FTP folder to This policy's destinations for that policy. See Figure 23 on page 28.

Establishing a Regular Migration Schedule

Migration activity to select files and copy them to secondary storage consumes resources which may impact overall system performance. You can avoid this performance impact during normal working hours by scheduling migration to occur outside of those hours. Copied files remain on disk for rapid access, but can be purged quickly when the managed file system is filled to a point where the remaining free space is less than the targeted free space or the file system becomes full. Purging has a negligible effect on performance.

Establish a regular migration schedule during those periods when network activity is at a low level. Migration operations at night, for example, can copy additional data from disk, making it possible for Storage Migrator to free file space quickly after user activity resumes the following morning. The objective is always to have enough files that can be purged on disk. This precludes Storage Migrator from initiating another file system sweep and copy operation when actual free space is less than targeted free space.

Migration Schedule Commands

The `migrate` command initiates a sweep of the specified file system(s). If no file systems are specified, Storage Migrator begins sweeping all managed file systems.

`migrate [`*`file system`*` [`*`file system`*`]]`

where *file system* is expressed as a disk drive partition, `D:` for example.

Use the `AT` command in Windows NT to execute the `migrate` command periodically.

`AT` ***`time`*** **`[/every:] [/next:]`** ***`command`***

Refer to your Windows NT documentation for the complete syntax and description of the `AT` command.

Procedure

1. Start the Schedule service. On the taskbar of your Windows NT desktop, click Start, and then point to Settings in the Start menu. Point to Control Panel in the Settings submenu. Double-click Services, and start the Schedule service.
2. Use the `AT` command to schedule periodic migration activity.

Example Migration Schedules

This example starts sweeping the managed file system on the `D:` disk at 2:00 AM every Tuesday, Thursday, and Saturday.

```
AT 02:00 /every:T,Th,S migrate D:
```

This example starts sweeping all managed file systems at 1:30 AM on the next Sunday.

```
AT 01:30 /next:Su migrate
```

This example starts sweeping the managed file systems on the `E:` and `F:` disk partitions at 10:00 PM every 5th and 20th of the month.

```
AT 22:00 /every:5,20 migrate E: F:
```

This example displays the status of current scheduled jobs.

```
AT
```

Typical output looks like this:

```
Status  ID  Day       Time      Command Line
-------------------------------------------------------------
        0   Each W    3:00 PM   C:\...\VERITAS\HSM\migrate.exe
        1   Each 24   2:30 PM   C:\...\VERITAS\HSM\migrate.exe
        2   Each Th   1:00 AM   C:\...\VERITAS\HSM\migrate.exe
```

Backing Up a Managed Store

Migrating files is not a substitute for backup. Storage Migrator detaches the data from migrated files when they are purged from disk. This migrated data in secondary stores cannot be used to reconstruct the file paths and access modes of the original files. Only backup software such as VERITAS NetBackup can back up and restore all files and the folder structure of the managed store.

Backup Schedule

Back up managed file systems and their databases on a regular schedule following the guidelines given here. This is a necessary to ensure migration data integrity when recovering from a catastrophic failure involving the Storage Migrator system. See “Recovering from a Disaster” on page 53.

Always back up a managed store, its databases, system registry, and local migration destination stores on the same schedule. Otherwise, the databases and registry will not correlate with the contents of the managed store after they are restored.

Scheduled backups can occur without interrupting migration activity. Storage Migrator automatically updates its databases to reflect any files that are migrated during the backup process.

Procedure

1. Establish a regular backup schedule for your system. VERITAS recommends that the longest interval between backups not exceed 24 hours.
2. Use VERITAS NetBackup to back up each managed store, its databases, system registry, and local migration destination stores. Use VERITAS NetBackup Database Extension for SQL to backup the VERITAS_HSM database.

Recovering from a Disaster

In the unlikely event of a catastrophic failure involving the Storage Migrator system, it is possible to restore the system to the status it had prior to the last backup of Storage Migrator's managed store, databases, system registry, and local migration destination stores.

This requires that you put in place a rigorous schedule of system backups. For optimum results, schedule these backups frequently. VERITAS recommends that the interval between backups not exceed 24 hours.

Backup Schedule

Use VERITAS NetBackup to back up and restore your managed file systems. Refer to your NetBackup system administrator's guide for detailed information on how to perform backups, archives, and restores.

The best approach is to configure your migration policies so no changed files are migrated before being backed up. There are two ways to accomplish this.

- Select the check box titled Migrate only files that are backed up in each migration policy (default). See Figure 15 on page 20.
- Otherwise, configure the Time since modified filter in the migration policies with a value equal to or greater than the longest scheduled interval between backups.

  For example, if your managed file system, databases, system registry and local migration stores are backed up every 24 hours, add a filter to one of the migration policies with the minimum time since file modification configured to be at least 24 hours. In this way, no changed files will be migrated before they are backed up at least once.

The restored file system, databases, system registry and local migration stores maintain data integrity with respect to the migrated data and, as with any file system not managed by Storage Migrator, only the work activity since the last backup needs to be repeated.

Backup Procedure

1. Establish a regular backup schedule for Storage Migrator's managed file system, databases, system registry and local migration stores.

   Use VERITAS NetBackup to back up each managed store, its databases, system registry, and local migration destination stores. Use VERITAS NetBackup Database Extension for SQL to backup the VERITAS_HSM database.

   See "Backing Up a Managed Store" on page 52.

2. Select the check box titled Migrate only files that are backed up in each migration policy (default), or configure the Time since modified filter in the migration policies with a value equal to or greater than the longest scheduled interval between backups.

3. Implement the regular backup schedule and continue it without interruption.

Disaster Recovery Procedure

Use VERITAS NetBackup to restore your managed file systems after experiencing a catastrophic failure involving the Storage Migrator system. Refer to your NetBackup system administrator's guide for detailed information on how to perform backups, archives, and restores.

After restoring all backed up information, staging resumes. All files previously migrated remain migrated, and will be staged if accessed. To resume migration, however, you must reconfigure each restored managed file system by selecting new migration attributes and assigning an existing or new policy set. This determines how Storage Migrator migrates files following the restoration, but does not affect staging of previously migrated files.

1. Format the disk partition on your system.

2. Restore the Storage Migrator-managed file system, databases, system registry and local migration stores using the most recent backup from NetBackup. Use VERITAS NetBackup Database Extension for SQL to restore the VERITAS_HSM database.

3. If reinstalling Windows NT, reinstall Storage Migrator.

4. Start the Storage Migrator service. On the taskbar of your Windows NT desktop, click Start, and then point to Settings in the Start menu. Point to Control Panel in the Settings submenu. Double-click Services, and start VERITAS Storage Migrator.

5. Bring up the Administration interface. On the taskbar of your Windows NT desktop, click Start, and then point to Programs in the Start menu. Point to VERITAS Storage Migrator in the Programs submenu, and then to the Administration icon.

6. Expand the Storage Migrator Server icon to reveal the file systems loaded on the server.

7. Select a restored managed file system and right-click its icon. Select Properties from the pop-up menu.

a. Set the two migration attributes on the File System dialog to their desired values. See “Set Migration Attributes” on page 16. Click Next. The Policy Set dialog appears.

b. In the Policy Set dialog, select an existing policy set from the drop-down list or click New to create a new policy set.

If you select an existing policy set and insert it in the Name field, click Finish to apply this policy set to the managed store.

If you create a new policy set, complete the Policy Set dialog and all subordinate dialogs. When you have included the desired number of policies in the new policy set, accept all open dialogs and return to the main screen to apply this policy set to the managed store.

8. Repeat the previous step for all restored managed file systems.

It is now possible to stage all previously migrated files and resume migration of new or modified files.

Using Storage Migrator Remote 4

This chapter explains operations that users may perform with Storage Migrator. Unless otherwise specified, the operations described here do not require root privileges.

As a user, automatic file migration and staging should satisfy most of your needs. During configuration, the administrator sets up Storage Migrator to automatically perform migrations in time to prevent you from running out of space. These migrations are transparent and should not affect your normal activities. File staging is automatic also and you continue to access files the same way, whether they are migrated or not. When you access a migrated file, the system transparently stages it for you; there is no difference in operation other than possibly a short delay. If the Storage Migrator service is not running when you access a migrated file, you receive an error message.

Although most user needs are taken care of automatically, Storage Migrator also allows you some control over file migrations and stages. For example, you can force Storage Migrator to migrate or stage individual files.

The topics in this chapter explain these user directed operations in more detail:

- Migrating Files
- Staging Files
- Identifying File Migration Status

All of these operations are initiated from Windows NT Explorer. Bring up Windows NT Explorer as follows:

1. On the taskbar of your Windows NT desktop, click Start, and then point to Programs in the Start menu.
2. Point to Windows NT Explorer in the Programs submenu.

Migrating Files

Storage Migrator adds functionality to Windows NT Explorer that enables users to migrate their own files.

These files are still subject to the cumulative effect of all of the policies in the policy set for the managed file system in which the file resides. A separate user migrate request is issued for each file selected.

Storage Migrator migrates one copy of the file to each destination store listed in each applicable policy. If no policies in the policy set apply to the file in the user migrate request, the file is not migrated. Storage Migrator does not re-migrate any selected files that already are migrated.

1. Make sure that the files you want to migrate are in a managed file system.
2. In the right pane of Windows NT Explorer, right-click one or more files you want to migrate.
3. In the drop-down menu, click Migrate.

Storage Migrator responds to these migration requests during its next migration operation.

Staging Files

Storage Migrator adds functionality to Windows NT Explorer that enables users to stage their own migrated files in advance of actually accessing them. A separate user stage request is issued for each file selected. Storage Migrator does not stage any selected files that already reside on disk.

1. In the right pane of Windows NT Explorer, right-click one or more files you want to stage.
2. In the drop-down menu, click Stage.

Storage Migrator responds to these stage requests during its next stage operation.

Identifying File Migration Status

Storage Migrator adds functionality to Windows NT Explorer that enables users to examine the migration status of files in managed file systems.

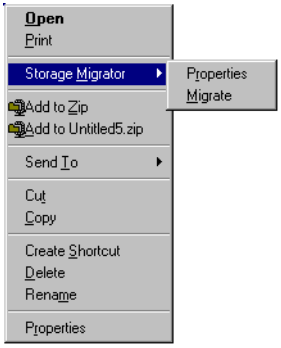
In the right pane of Windows NT Explorer, icons of migrated files contain a black “offline” overlay in the lower left corner to indicate their migrated status. Icons of unmigrated files do not contain this overlay.

You can obtain additional information about a file’s migration status, number of copies and their location, and file properties by following the next procedure. For multiple files, see “Status of Multiple Files” on page 60.

Status of a Single File

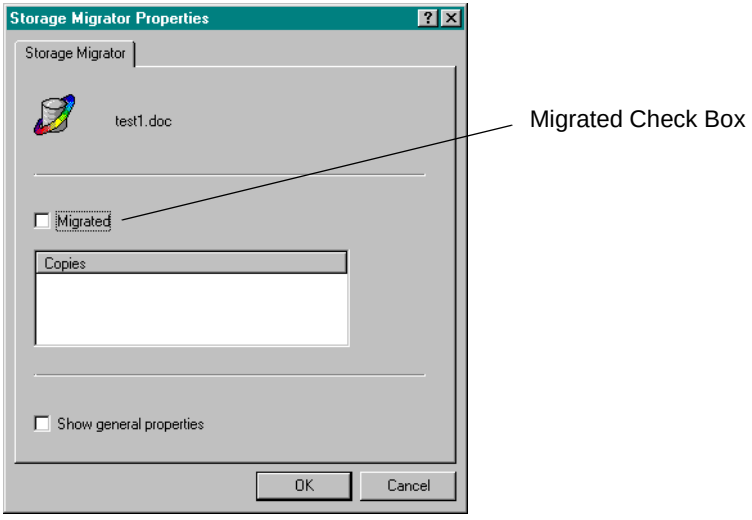
1. In the right pane of Windows NT Explorer, right-click a file you want to identify.
2. In the drop-down menu, click Storage Migrator and then Properties.

Figure 39. Menu Choices



The Storage Migrator Properties dialog appears.

Figure 40. VSM Properties Dialog, Single File

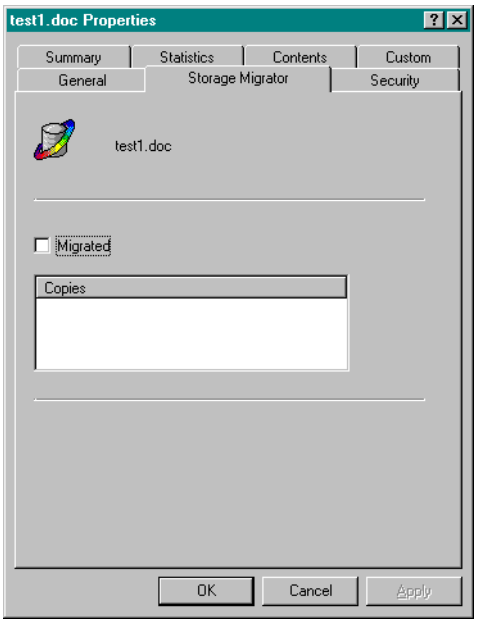


If the Migrated check box is not selected, the file resides on disk. To migrate the file, click to select the Migrated check box.

If the Migrated check box is selected, the file has been copied and purged so it no longer resides on disk. To stage the file, click to select the Show general properties check box.

The file Properties dialog appears. Click the Storage Migrator tab.

Figure 41. File Properties Dialog, Single File



Storage Migrator stages migrated files to determine their general properties. Thus, the file resides on disk, and the Migrated check box is not selected on the file Properties dialog. To migrate the selected file, click to select the Migrated check box.

Note Existing file copies and their location are also listed in these dialogs.

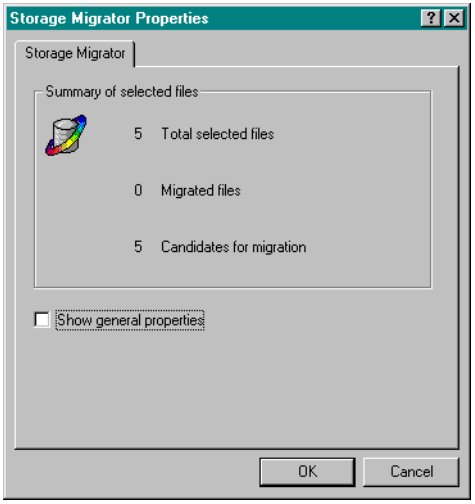
3. Click OK or Cancel to close the dialogs.

Status of Multiple Files

1. In the right pane of Windows NT Explorer, right-click the files you want to identify.
2. In the drop-down menu, click Storage Migrator Properties.

   The Storage Migrator Properties dialog appears.

Figure 42. VSM Properties, Multiple Files



This displays a summary of how many of the selected files are migrated or could be migrated.

To stage the selected migrated files, click to select the Show general properties check box.

The file Properties dialog appears. Click the Storage Migrator tab.

Storage Migrator stages migrated files to determine their general properties. Thus, the files reside on disk, and the Migrated check box is not selected on the file Properties dialog. To migrate all of the selected files, click to select the Migrated check box.

Note Existing file copies and their location are not listed in these dialogs.

3. Click OK or Cancel to close the dialog.

Moving Storage Migrator Remote for Windows NT A

Introduction

This document describes the procedure to move Storage Migrator Remote for Windows NT from an existing computer to a new computer that will also run Storage Migrator Remote.

The basic steps are

- Determine the needed configuration of the *destination* computer.
- Move the VSM database and file systems to the *destination* computer.
- Move the VSM configuration information from the *source* computer to the *destination* computer.
- Start running storage migrator on the new computer.

Caution The *source* computer must be running the same version of VSM that will be installed on the *destination* computer.

Note You must be logged in with administrative rights on the *source* and *destination* computers to complete this procedure.

Abbreviations Used in this Procedure

In the following procedure, we will use the following abbreviations:

- *VSM* means *Storage Migrator Remote for Windows NT.*
- *Source* means the *computer using VSM to manage its file systems, where the file systems move from.*
- *Destination* means the *computer where the file systems on the source moves onto.*

Moving *VSM* to a New Computer

How to Move *VSM* to a New Computer

Note You must be logged in with administrative rights on the *source* and *destination* computers to complete this procedure.

1. Determine necessary configuration for file systems on the *destination* computer.

   a. For each managed NTFS file system on the *source* computer, identify a corresponding NTFS file system to manage on the *destination* computer. Each file system on the new computer should be at least as large as the one it is replacing on the new computer.

Note Drive letters on *source* and *destination* do not have to match.

   b. From a DOS command prompt on the *source* computer, run the **`migattr liststores`** command. For each managed file system, there will be a corresponding file system ID. When you do this, you will see output that looks something like the following.

      For example:

      C:> Program Files\VERITAS\Hsm\migattr liststores

      A: [NOT ENABLED]

      B: [NOT ENABLED]

      C: [NOT ENABLED]

      D: [NOT ENABLED]

      E: [f6787643-21bd-11d4-92fd-0060b07b8ce5]

      F: [NOT ENABLED]

      G: [f678766e-09ac-11d4-92fd-0060b07b8ce5]

      H: [NOT ENABLED]

   c. Record the *source* managed file system drive letter, *destination* drive letter, and *source* file system system ID for each managed file system.

      In this example, we are moving managed file system E: on the *source* to H: on the *destination*, and G: on the *source* to L: on the *destination*.

source **managed file system drive letter**	***destination*** **drive letter**	***source*** **file system ID**
E:	H:	f6787643-21bd-11d4-92fd-0060b07b8ce5
G:	L:	f678766e-09ac-11d4-92fd-0060b07b8ce5

2. Determine the path to install *VSM*, along with SQL server database tables, on the *destination* computer.

a. You will need a drive on the *destination* with space for the VERITAS_HSM database. The database will be installed on the same drive as *VSM*.

b. You'll need at least as much space for the database on the new (*destination*) computer as on the *source* computer. To see how much space the database uses on the *source* computer, find the location of the VERITAS database by looking at the properties display for your server from the VSM Administrative interface. The minimum amount of space you'll need for the new database on the *destination* is at least the size of *vxhsm.mdf + vxhsm.log*.

Note You should allow additional space for the database to grow as more files are added.

3. Stop the *VSM* Service on the *source* computer.

- Stopping the *VSM* Service, prevents file system further migration and database changes.

4. Backup each *source* managed file system.

- Do an alternate restore of each file system, on the *source*, to the corresponding drive on the *destination*.

Note Drive letters on *source* and *destination* can be different.

5. Install *VSM* on the *destination*.

a. Install *VSM* on the *destination* computer.

b. Reboot the *destination* computer.

c. Stop the *VSM* Services. To do this, select services from the control panel. This step will install *VSM*, along with an initial empty database, on the new (*destination*) server.

6. Copy the *source* database to the *destination*.

   a. Use the NetBackup client extension for Microsoft SQL Server to backup the *source* VERITAS_HSM database. Then, complete an alternate database restore to the *destination*.

   b. If you do not have the NetBackup client extension for Microsoft SQL Server, VERITAS can supply you with a command line utility to export the database from the *source* and move it to the *destination*.

7. Copy the *VSM* store configuration through the registry. This step copies the configuration for Stores, Filters, Policies, and PolicySets from the *source* computer to the *destination*. You will export four registry keys from the *source* computer, and import them to the registry on the *destination* computer.

   a. On the *source* computer, run **`regedit`**. Open `HKEY_LOCAL_MACHINE \ SOFTWARE \ VERITAS \ HSM \ CurentVersion \ Store`. From the Registry menu, click on Export Registry Key. Export the registry key as '*stores*.' Run the file you have created (*stores.reg*) on the *destination* computer. This will copy the VSM Stores configuration from the *source* computer to the *destination* computer.

   b. Repeat the process described in step a on the path below, but create a file named *policy.reg* from the *source* registry, and run it on the *destination:*
   `HKEY_LOCAL_MACHINE \ SOFTWARE \ VERITAS \ HSM \ CurentVersion \ Policies`

   c. Repeat the process described in step a on the path below, but create a file named *PolicySet.reg* from the *source* registry, and run it on the *destination*.
   `HKEY_LOCAL_MACHINE \ SOFTWARE \ VERITAS \ HSM \ CurentVersion \ PolicySet`

   d. Repeat the process described in step a on the path below, but create a file named *Filter.reg* from the *source* registry, and run it on the *destination*.
   `HKEY_LOCAL_MACHINE \ SOFTWARE \ VERITAS \ HSM \ CurentVersion \ Filter`

8. Setup the managed file system store ID on the *destination* to match the *source*.

   - On the *destination*, from the DOS command prompt, run **`migattr hsmenable`** to setup the managed file system store ID to match the *source*.

     For example, the commands set the file system ID and enable VSM on drives H and L on the *destination*. The file system IDs in the following example came from the **`liststores`** command done in step 1 on page 64.

     C:> Program Files\VERITAS\Hsm\migattr hsmenable H:\ f6787643-21bd-11d4-92fd-0060b07b8ce5

     C:> Program Files\VERITAS\Hsm\migattr hsmenable L:\ f678766e-09ac-11d4-92fd-0060b07b8ce5

Note Exact command syntax is important! Note the '\' following the drive letter.

9. Restart *VSM* service on the *destination*.

- To restart *VSM* service on the *destination*, select services from the control panel. Then, start the Veritas Storage Migrator Remote service.

10. Verify that you can stage migrated files and migrate files from each file system.

Filter Units of Measurement B

Introduction

The following topics are discussed in this appendix:

- Filter Units of Measurement

Filter Units of Measurement

The following multipliers are used to calculate the units of measurement for policy filters.

Size Units

1 byte
1 kilobyte (1,024 bytes)
1 megabyte (1,024 kilobytes = 1,048,576 bytes)
1 gigabyte (1,024 megabytes = 1,073,741,824 bytes)
1 terabyte (1,024 gigabytes = 1,099,511,627,776 bytes)

Time Units

1 second
1 minute (60 seconds)
1 hour (60 minutes = 3600 seconds)
1 day (24 hours = 86400 seconds)
1 week (7 days = 604,800 seconds)
1 month (30 days = 2,592,000 seconds)
1 year (365 days = 31,536,000 seconds)

Running Storage Migrator Remote on MSCS Cluster Failover C

Overview

This appendix explains how to install and configure VERITAS Storage Migrator Remote for Windows NT (Cluster Edition) in a MSCS cluster environment.

In this appendix, Storage Migrator Remote for Windows NT (Cluster Edition) is also referred to as *VSM Cluster*. For a list of terms used in this appendix see “Glossary of Terms” on page 81.

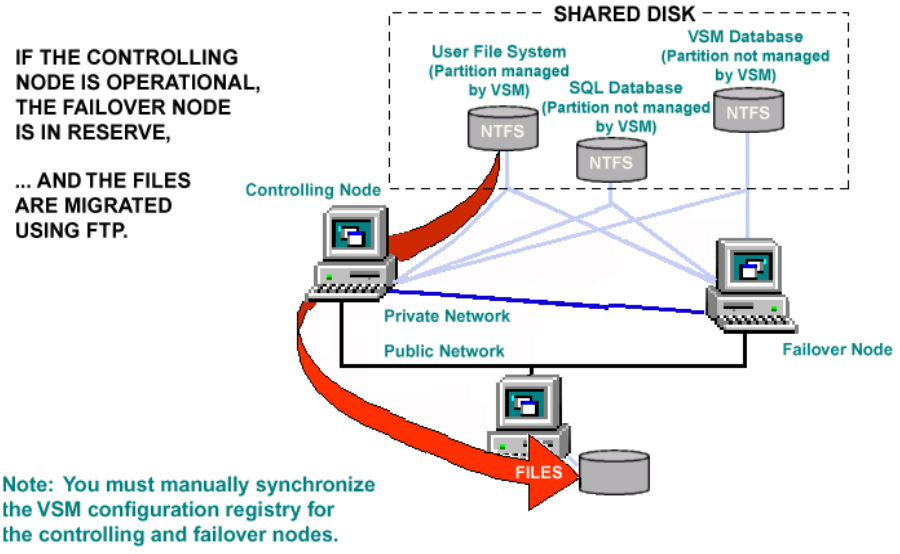
VSM has been tested running with MCSC Cluster and failover. VSM Cluster increases availability by having a secondary server manage file systems if the primary server goes down.

The VSM database contains information needed by VSM to locate migrated files. Each node contains the VSM configuration in the Windows NT registry. When configuring VSM, you manually copy (synchronize) this VSM registry from the controlling node to the failover node.

The following two sections illustrate how VSM Cluster seamlessly migrates data in normal and failover modes.

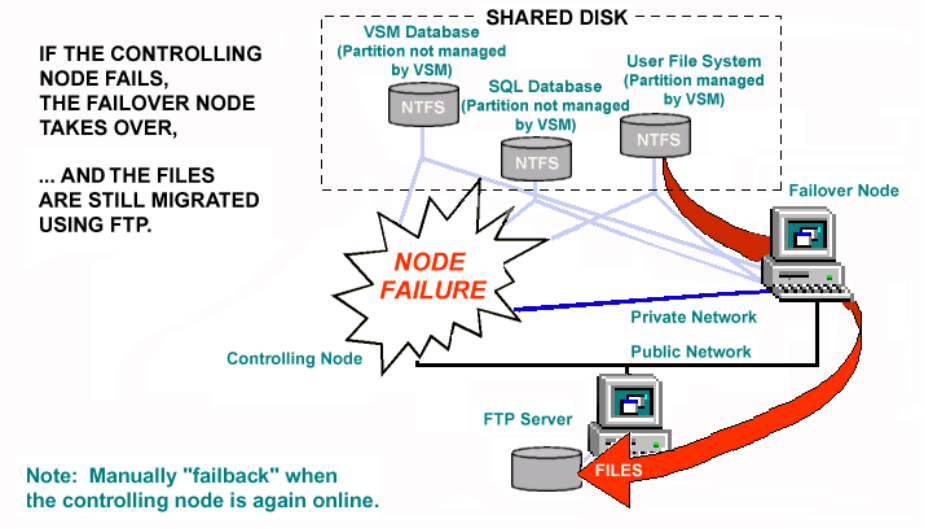
VSM Cluster Normal Functionality

The following typical configuration shows VSM Cluster functionality, when both nodes are operating normally.



VSM Cluster Failover Functionality

The configuration in the following figure shows VSM cluster failover functionality, which results when the controlling node has a failure and the failover node resumes VSM operations.



After a failover and the controlling node is online, you should manually failback VSM operations to the controlling node.

Note You must manually synchronize the VSM configuration registry on both nodes, if any configuration changes occur.

If you want to choose a local folder as the destination for the migration, the destination for the local folder has to be on the shared disk.

Operational Notes

Keep the following points in mind when running VSM Cluster:

- Running VSM Cluster requires a working knowledge of the Microsoft software products listed under “Software Requirements” on page 75.
- Partially staged files might need to be re-staged after failover.
- If a failover occurs during a migration sweep, the failover node will restart the migration sweep.
- Microsoft recommends that you manually complete failback.
- Install SQL Server 7.0 Enterprise Edition from the controlling node in the cluster (SQL Server should be installed to a partition on the shared disk). Each node will have SQL Server information in the registry.
- VSM only supports SQL Server Active / Passive failover (SQL Server is installed on the controlling node only).

Requirements

Hardware Requirements

The following are hardware requirements for VSM Cluster:

- Two identical computers. Check the Microsoft web site for the Hardware Compatibility List (HCL).
- Two network adapters for each computer.
- SCSI disks.
- Crossover network cables to establish the private network for interconnect.
- All shared disks must be configured as *basic* (not dynamic).
- All drive partitions on shared disks must be formatted as NTFS. The shared disk must have at least two partitions as follows:
  - One or more partitions for user data. This data can be one or more file systems that are managed by VSM.
  - One partition containing the VSM installation and SQL Server. These file systems are *not* managed by VSM.

VSM Cluster has been tested on SCSI disks using crossover network cable. For better performance and failover factor, Microsoft recommends using RAID disk, fibre channel.

IP Address and Network Name Requirements

Seven unique, static IP addresses are used for setting up VSM Cluster as follows:

- Two IP addresses and network names for network adapters on the public network are used by two identical computers.
- Two IP addresses for network adapters on the private network are used by two identical computers for interconnect.
- One IP address and network name is used to set up a cluster (see "1. MSCS Set Up" on page 76).
- One IP address and network name is used for setting up MSDTC (see "Preparation of Cluster Resources for MSDTC" on page 77).
- One IP address and network name is used to set up a SQL Server virtual server (see "SQL Server Cluster Service Set Up" on page 78).

Each of the two computers has the following IP addresses:

- A private IP address for network adapters on the private network used by MSCS Cluster.
- A public network IP address and network name for network adapters on the public network.

Software Requirements

The following are the software requirements for VSM Cluster:

- Microsoft Windows NT 4.0 Enterprise Edition.

  Only Windows NT 4.0 Enterprise Edition supports MSCS Cluster. If you want to run VSM Cluster, you must upgrade to Windows NT Server Enterprise Edition with the MSCS add-on.
- Microsoft Windows NT Service Pack 6a.
- Microsoft Internet Explorer 4.01 Service Pack 1 (or greater) and MDAC 2.0.
- Microsoft SQL Server 7.0 Enterprise Edition.
- Microsoft SQL Server Service Pack 2.
- MSCS (Microsoft Cluster Server).
- MSCS Cluster Administrator.
- VERITAS Storage Migrator Remote 3.4.1 for Windows NT (Cluster Edition).

Environment Configuration Tasks

Complete these configuration tasks in the order shown.

If you already have MSCS Cluster installed, you can start with step 2. The software requirements remain the same, see page 75.

If you already have MSCS Cluster and SQL Server installed, you can start with step 3. Make sure that SQL Server and VSM are on the same disk group (see "Preparation of Cluster Resources for MSDTC" on page 77 and "4. VSM Cluster Set Up" on page 80). The software requirements remain the same, see page 75.

1. MSCS Set Up
2. SQL Server Installation and SQL Cluster Failover Set Up
3. VSM Installation and Configuration
4. VSM Cluster Set Up
5. Verify the VSM Cluster Set Up
6. Verify VSM Cluster Failover

1. MSCS Set Up

This step requires the Windows NT 4.0 Enterprise Edition CD and includes the following tasks:

- Installing and configuring MSCS on the controlling and failover nodes.
- Setting up the cluster with at least two partitions (shared drives) on the shared disk.
- Setting up the two nodes as a cluster.

See Chapter 3 - Setting Up an MSCS Cluster, in the *Microsoft Cluster Server Administrator's Guide* for instructions for these tasks. This guide is available on the Windows NT 4.0 Enterprise Edition CD.

2. SQL Server Installation and SQL Cluster Failover Set Up

Using VSM Cluster requires MS SQL Server running on the cluster. SQL Server must be installed to a partition on the shared disk and must be installed from the controlling node.

The following table provides an overview of the steps and the nodes involved. These steps require the Storage Migrator Remote 3.4.1 for Windows NT (Cluster Edition) CD.

Both nodes must be up and running.

Perform this Step	On the Controlling Node	On the Failover Node
Preparation of Cluster Resources for MSTC.	Yes	
SQL Server Installation.	Yes	
SQL Server Service Pack 2 Installation.	Yes	Yes
SQL Server Cluster Service Set Up.	Yes	
Reboot Node.		Yes

For the installation and configuration instructions needed to complete these steps, see the *Microsoft SQL Server - How to Install SQL Server 7.0, Enterprise Edition on Microsoft Cluster Server: Step by Step Instruction*.

Caution VSM must not be configured to manage the file system where SQL Server is installed.

Preparation of Cluster Resources for MSDTC

This involves the preparation of the cluster resources to use SQL Server, and requires one unique IP address and a network name.

1. From the MSCS Cluster Administrator on the controlling node, choose a disk group and rename it (for example, you could use *VSM Cluster* as the name).
2. Create MSDTC IP Address and MSDTC Network Name cluster resources.

SQL Server Installation

1. Make sure that the controlling node is the active node (is the owner of the shared disk).
2. Install SQL Server 7.0 Enterprise Edition from the controlling node. When prompted for a 10-digit key for the CD, enter all 9s.

   All major SQL Server files are installed on the controlling node and the necessary SQL Server files are automatically installed on the failover node.

SQL Service Pack 2 Installation

1. From the VSM CD Autorun screen on the controlling node, install SQL Server Service Pack 2.
2. Make the CD drive a shared drive (for use in the installation on the failover node—step 3).
3. From the VSM CD Autorun screen on the failover node, install SQL Server Service Pack 2 from the CD shared drive.

SQL Server Cluster Service Set Up

This step requires one unique IP address and network name to set up a SQL Server virtual server.

- From the VSM CD Autorun screen on the controlling node, run the SQL Server cluster service setup.

Reboot Node

- Reboot the failover node after completing the installation.

3. VSM Installation and Configuration

VSM is installed on both the controlling node and the failover node. VSM must be installed to a partition (shared drive) on the shared disk, and must be installed to the same path from the controlling and the failover nodes.

The VSM database will also be stored at this location on the partition. Make sure there is enough disk space for the VSM database to expand.

Caution VSM must not be configured to manage the file system where VSM is installed.

These steps require the Storage Migrator Remote 3.4.1 for Windows NT (Cluster Edition) CD.

On the Controlling Node

1. Install VSM to the shared disk.
   a. From the MSCS Cluster Administrator, make sure that the controlling node is the active node (is the owner of the shared disk).
   b. Log in as the administrator on the Windows NT server or workstation where you are going to install VSM.
   c. Close all applications and disable any virus detection software.

d. Use the normal VSM installation (you can use `setup.exe` or Autorun).

e. Reboot the node.

f. From Services in the Windows NT control panel, set up the VSM service to start up manually.

2. Using the VSM Administration GUI, set the VSM database server to be the SQL Server virtual server. Use the network name you used to set up the cluster service in "SQL Server Cluster Service Set Up" on page 78.

a. From the Edit menu, select Properties.

Enter the name of the VSM database server in the Database Server box. Click OK.

b. From Services in the Windows NT control panel, stop and restart the VSM service.

3. Configure VSM managed file systems and stores.

See the "Configuration Process" on page 14 to configure the managed file system.

4. Export the configuration.

a. From a DOS command line, go to the VSM installation path.

b. Run `VSMConfig -export`.

On the Failover Node

1. Install VSM to the shared disk.

a. From the MSCS Cluster Administrator, make sure that the failover node is the active node (is the owner of the shared disk).

b. Log in as the administrator on the Windows NT server or workstation where you are going to install VSM.

c. Close all applications and disable any virus detection software.

d. Use the normal VSM installation (you can use `setup.exe` or Autorun). Use the same installation path on the shared disk as was used when installing VSM on the controlling node.

e. Reboot the node.

f. From Services in the Windows NT control panel, set up the VSM service to start up manually.

2. To synchronize the configuration, import the configuration.

a. From a DOS command line, go to the VSM installation path.

b. Run `VSMConfig -import`.

Note If you change the VSM configuration on the controlling node, you must synchronize the VSM configuration on the failover node. Run `VSMConfig -export` on the controlling node and then run `VSMConfig -import` on the failover node.

4. VSM Cluster Set Up

Complete the following steps from MSCS Cluster Administrator to add the VSM services to the disk group (for example, *VSM Cluster*) that you created earlier in "Preparation of Cluster Resources for MSDTC" on page 77.

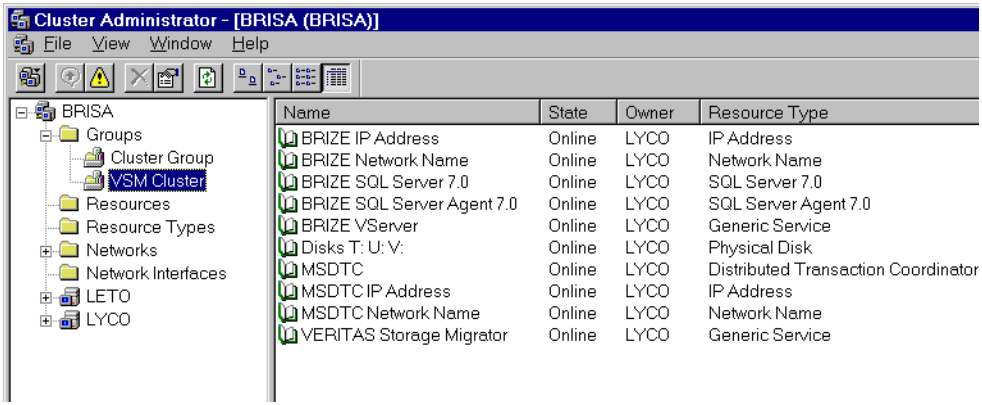
1. Configure the controlling node to be the active node.
2. Click new and then resource, choose Generic Services for the resource type, enter VxHSMService for Service name on the Generic Service Parameters, and choose dependencies.
3. Click finish on the dialog box.

   When configured correctly, VSM Cluster will failover automatically.

5. Verify the VSM Cluster Set Up

After you configure VSM Cluster, a resource list is displayed on the MSCS Cluster Administrator. In the resource list example that follows:

- VSM Cluster is the disk group name you used in "Preparation of Cluster Resources for MSDTC" on page 77.
- BRIZE is the SQL Server virtual server network name you set up in "SQL Server Cluster Service Set Up" on page 78.
- Disks T, U, and V are the partitions on the shared disk you set up in "1. MSCS Set Up" on page 76.
- MSDTC is the name that is automatically generated during the SQL Server installation.
- MSDTC Address and MSDTC Network Name were set up in "Preparation of Cluster Resources for MSDTC" on page 77.



6. Verify VSM Cluster Failover

On the managed file system, all files that meet the VSM migration policy are migrated out to the destination.

1. If there are no files on the managed file system, copy several files to the file system for testing to verify migration, caching, and failover.
2. Verify that you can cache a migrated file on the controlling node.
3. Shut down the controlling node (the owner of the shared disk). All resources should automatically move to the failover node.
4. Verify that you can cache a migrated file on the failover node.

Glossary of Terms

Cluster - Two computer systems addressed and managed as a single system.

Controlling Node - The node used to process all client resources and workload. The idle companion node is called a *failover node.*

Failover - Process of switching from the controlling node to the failover node.

Failback - Process of switching back to the original controlling node after a failover.

Failover Node - The node used to recover the resources and workload if the controlling node in the cluster fails. This node is often idle because the controlling node is working.

Interconnect - Private network that connects the controlling and failover nodes in a cluster.

MSCS - Microsoft Cluster Server.

MSDTC - Microsoft Distributed Transaction Coordinator.

SQL Server - Microsoft SQL Server.

VSM - VERITAS Storage Migrator Remote for Windows NT.

VSM Database - A SQL Server database that contains information used by VSM to track migrated files.

VSM Cluster - VERITAS Storage Migrator Remote for Windows NT (Cluster Edition).

Glossary

Administration interface
The Storage Migrator administrator graphical user interface.

Administrator Station
A Windows NT system running the Storage Migrator administrator graphical user interface (Administration interface).

API
Application programming interface.

archive
The process of backing up files and directories to a storage unit and then deleting the original files and directories.

attribute (policy)
That part of a policy which is specific to the policy type.

backup
The process of copying and saving files and folders to storage media.

cache - see *stage*

concurrent recording
The process of copying data to more than one storage device at the same time.

destination (policy)
That part of a policy which defines *where* the data from files subject to the policy is copied.

destination store - see *secondary store*

directory - see *folder*

file migration - see *migrate*

file staging - see *stage*

file system store
A primary store managed by Storage Migrator.

filter (policy)
That part of a policy which defines *which* files are subject to the policy.

first-level migration
The process of copying data from a managed file system to a secondary store. See also *migrate*.

folder
A collection of programs, files, or other folders within a file system.

folder store
A folder accessible from the Storage Migrator Server that is used as a store.

free space
The space in the managed file system that is unused.

FAT
File Allocation file system.

FTP
File transfer protocol.

FTP Server
A remote server (Windows NT, UNIX, or other) accessible through standard FTP protocol.

FTP store
A folder on an FTP server accessible through standard FTP protocol that is used as a store.

GUI
Graphical user interface. Also referred to as an *interface*.

hierarchical storage management
The process of automatically migrating selected files from a managed file system to specified migration levels on secondary storage while maintaining transparent user access to those files.

HSM
This is an abbreviation that represents both VERITAS Storage Migrator and VERITAS Storage Migrator Remote; may also be referred to as *VSM*. See also *Hierarchical Storage Management*.

interface
Graphical user interface. Also referred to as a *GUI*.

I/O
Input/output.

managed file system
A file system managed by Storage Migrator.

managed store
A store configured to have a policy set applied to it.

migrate
The process of copying file data to secondary storage and then purging the data from disk while retaining the file names and file structure in the managed file system. See also *Targeted free space*.

Migration preference
A configurable migration parameter that weighs file size and file age in determining which files are copied to secondary storage first.

NTFS
Windows NT File System.

policy
The configurable specifications that define the exact operations Storage Migrator performs on a managed store.

policy set
A collection of policies applicable to a particular managed store.

primary store
A store directly accessible by a user, such as a file system.

purge
The process of deleting migrated file data from disk after all copies have been made. See also *Targeted free space*.

secondary store
A store, not directly accessible by a user, to which Storage Migrator stores copies of data, such as a folder.

stage
The process of copying migrated files back to the managed file system for access.

staging delay
The period between the time a **`read`** or **`write`** request is issued and the time the migrated file is accessible, during which Storage Migrator stages the file from a secondary store.

Storage Migrator Remote Server
A Windows NT system with file systems managed by Storage Migrator.

store
A set of like media used to hold copies of file data. See *primary store*, *secondary store*.

targeted free space
: The amount of file system capacity on disk that Storage Manager tries to maintain as not utilized.

threshold
: A disk utilization level beyond which Storage Migrator operations occur. See *Targeted free space*.

User Station
: A Windows NT system running the Storage Migrator end user interface with shell extensions to Windows NT Explorer.

VSM
: This is an abbreviation that represents both VERITAS Storage Migrator and VERITAS Storage Migrator Remote; may also be referred to as *HSM*. See also *Hierarchical Storage Management*.

Index